INTERNET GOVERNANCE AND REGULATIONS IN LATIN AMERICA

Analysis of infrastructure, privacy, cybersecurity and technological developments in honor of the tenth anniversary of the *South School on Internet Governance*

Luca Belli and **Olga Cavalli**
Editors

Prefaces by **Vinton G. Cerf** and **Raúl Echeberría**

Postface by **Edison Lanza**

ssig South School on internet Governance

ccat lat CENTRO DE CAPACITACIÓN EN ALTA TECNOLOGÍA PARA LATINOAMERICA Y EL CARIBE

Internet Society

FGV DIREITO RIO

lacnic

Internet Governance and Regulations in Latin America

Analysis of infrastructure, privacy, cybersecurity and technological developments in honor of the tenth anniversary of the *South School on Internet Governance*

The original versions of the chapters of this book were drafted in Spanish and Portuguese. Please, refer to the original versions to solve any doubts that might arise in case of excessively loose translations.

Edition produced by FGV Direito Rio
Praia de Botafogo, 190 | 13º andar
Rio de Janeiro | RJ | Brasil | CEP: 22250-900
55 (21) 3799-5445
www.fgv.br/direitorio

Internet Governance and Regulations in Latin America

Analysis of infrastructure, privacy, cybersecurity and technological developments in honor of the tenth anniversary of the *South School on Internet Governance*

Luca Belli and *Olga Cavalli*
Editors

Prefaces by *Vinton G. Cerf* and *Raúl Echeberría*
Postface by *Edison Lanza*

EDITION FGV Direito Rio

Printed in Brazil
Completion of the First Edition in September 2019

Coordination: Rodrigo Vianna, Sérgio França e Thaís Mesquita

Cover: Andreza Moreira – Tangente Design

Layout: Andreza Moreira – Tangente Design

Review: Olga Cavalli, Luca Belli and Walter Britto

Translation: Central de Traduções & Global Languages

Cataloguing data prepared by the Mario Henrique Simonsen/FGV Library

Internet governance and regulations in Latin America : analysis of infrastructure, privacy, cybersecurity and technological developments in honor of the tenth anniversary of the South School on Internet Governance / Luca Belli and Olga Cavalli, editors; prefaces by Vinton G. Cerf and Raúl Echeberría; postface by Edison Lanza. - Rio de Janeiro : FGV Direito Rio, 2019.
526 p.

Includes bibliography.
ISBN: 978-85-9597-036-6

1. Internet governance. 2. Data protection. 3. Internet – Cybersecurity. 4. Information Technology. I. Belli, Luca. II. Cavalli, Olga. III. Getulio Vargas Foundation Rio de Janeiro Law School.

CDD – 384.3

CONTENTS

PREFACE

Internet Governance Issues and Challenges in the Americas

Vinton G. Cerf

I am honored to write this foreword to an important and timely book on the challenges posed by today's Internet. The primary themes of the book cover a substantial amount of territory, all of which is relevant as we consider how the Internet is to be governed. Historically, the system has evolved in a collaborative and global fashion and it is reasonable to assume that this narrative will continue to characterize the system. The Internet is made up of independent networks operated by different parties with a variety of business models.

There are no rigid rules for interconnection other than the bilateral decisions of operators to interconnect on mutually acceptable terms and conditions. In some jurisdictions, there are concerns about adequate competition; especially among broadband Internet access providers, leading to debates on the neutrality of access provision[1]. Providers are urged not to interfere with consumer choices or to meddle with the performance of the system to favor one or another application provider.

The sections of this book mirror current concerns shared by many who are part of the Internet community: Inclusiveness of access, protection of personal information, safety and security when using online services and the effects of disruptive technologies that may upend earlier business models. Each of these topics raises significant governance questions that are relevant not only to the Americas, but to every part of the world where Internet is accessible and, especially, where it is not yet available.

Regarding Internet access, the primary objectives should be that the Internet be accessible, affordable, reliable and useful. These are non-trivial goals and raise many questions about technology,

1 See <https://www.networkneutrality.info>.

business models, content, and literacy. For example, oral interaction with the Internet may overcome local limitations in written literacy. This technology (speech recognition and processing) is becoming increasingly available and reliable. The rapid proliferation of mobile technology, especially *smart phones*, has delivered Internet access to billions who might otherwise never have had convenient access. There is no question that increased access speeds have enabled new applications and businesses to emerge, including streaming audio and video, video conferencing, interactive games, digital book distribution and convenient electronic commerce including purchase of goods and services, online advertising, online auctions, and a host of other capabilities.

Today's online environment affords access to enormous quantities of information of highly varying quality. Search engines index the contents of the network, primarily the World Wide Web, and assist users to find information of interest. While the ranking of search results represents an attempt by the search engines to present information from most relevant to less relevant, users are still challenged to discover information they consider useful. The ability to search through vast quantities of content challenges notions of privacy thanks to the ever-present smart phones, laptops and tablets with their high resolution cameras and applications that allow users to send email, "tweets," social media messages and to upload images, texts and videos to information sharing sites. Facial recognition programs, intended to help users catalog and sort their personal photographs, also can be used to search the Web for virtually anyone for whom the user has an identified photo.

This means that casual photos not intended to highlight innocent bystanders may still be found and labeled. Even without such recognition mechanisms, one might be searching for one thing and discover information, images, or videos of someone they know but were not looking for. Social media sharing, "tagging" of images and unauthorized uploads of personal information make it increasingly difficult to achieve any sort of privacy. While laws such as the General Data Protection Regulation (GDPR) of the European Union attempt to protect personal information, it is very hard to avoid the sense that privacy is very difficult to maintain in

the 21st Century. Plainly, work is needed on the policy and technical sides to give users tools to understand how online services work and protect their privacy.

Among the most effective business models in the present Internet is advertising based services in which users get free application services in exchange for exposure to selected advertisements. This was the backbone of the news business, but the online environment is even more powerful because the advertisements can be chosen to match perceived user interests – unlike the fixed advertisements found in television, radio, newspapers and magazines. However, to target particular ads to particular users requires knowledge of user interests, which may be indicated by searches of the Web, expressions found in social media and even explicit indications from users of products or services of interest to them. For some users, this method of selective advertising feels privacy invading and adds to the sense that privacy may be very hard to achieve if one is technically uneducated and is making significant use of free, online service.

When the Internet was created, among the driving motivations was to drop barriers to sharing of and access to information. In large measure, this objective has been achieved for at least half the world's population. As the Internet has become accessible to the general public, it has become apparent that the barriers to bad or even illegal behavior have dropped, resulting in a significant amount of troublesome content and behavior deemed to be harmful to society. Fraud, harassment, bullying, malware, denial of service attacks, child pornography, disinformation, "fake news," "alternative facts" and a host of other objectionable content is being injected into the network along with high quality information from trusted sources.

Of particular concern is malicious software (better known as "malware") that is intended to break into systems, steal important information (e.g. passwords, account and credit information and personal information suitable for identity theft) or otherwise disrupt the operation of systems relying on the online environment to function. These are serious hazards with the potential to cause serious damage to commerce and infrastructure, to spread

misinformation and rumors, and generally create a wide range of disruption. The fact that we have become increasingly dependent on our online ecosystem exacerbates the risk that these attacks pose. Responses to cyber-attack must be very carefully thought through – false flag attacks could lead to massive diplomatic blunders and even international conflict. Automated responses that damage attacking computers could accidentally cause collateral damage to the equipment of innocent bystanders whose laptops or mobiles have been invaded and made part of a so-called "botnet" used to generate spam, distribute malware, or launch denial-of-service attacks. Coping with this class of problems will require serious research and creative transnational diplomatic efforts to inhibit, or at least mitigate the effects, and identify perpetrators so that action against them can be taken.

Finally, one must face the fact that new technologies displace old ones, and this may have the side-effect of upending old business models. When costs drop dramatically or time to reach the market is compressed or productivity and customization replace older production models, there can be serious economic consequences. There is an old expression: "If someone is going to eat your lunch, it might as well be you!" By this, one means that it is better to compete with your own products rather than letting someone else undermine your market using new technology. Anticipating the effects of new technologies is never easy but this is precisely what is needed to prepare for changing business environments that demand adaptation. Darwin was right: "Adapt or die!" Machine learning and artificial intelligence are simply two of the most recent innovations with potentially massive impact on existing businesses.

This book is intended to help readers cope with the rapidly evolving environment of online communication and the concomitant application of computing technology to practically everything. This is particularly important for policy makers to understand and appreciate because their regulatory and enforcement environments will be significantly affected by the new technologies that are emerging thanks to the rich research and development environment that is fed, in part, by the online Internet information space and its rapidly growing computational capacity.

PREFACE

Building Innovative Governance Models

Raúl Echeberría

We live in fascinating times in relation to the growth of the Internet in the world.

The Internet is an intrinsic component of all human activities; more than half of the world's population is already connected to it.

The impact of the Internet on the world is enormous, which generates a first challenge for us: to reduce the gap in opportunities between those who are connected, and those who are not.

Everything those of us who have Internet access do naturally every day (pay an account, buy something, buy tickets for a concert, make a work conference, sell a service, or send a message to the family…) are things that are available only for a little more than half of the world's population.

The world works under the premise that everyone is connected, but that, unfortunately, is not true. Therefore, the great challenge is to connect everyone in a way that connectivity affects people's lives in a positive way and at a reasonable time. In other words, that the Internet of opportunities becomes a reality for everyone.

Another effect of the constant development of the Internet is the growing interest from the political point of view. As the role of the Internet has increased in all aspects of society, it is natural that the attention and concern of governments and other actors about the various impacts of this new reality on the world we know, also increases.

Around the world, we can see intense debates on several Internet-related topics including the impact of the digital economy on local economies, the impact of artificial intelligence on the labor market, the application of existing tax frameworks to new business models, the challenges of cybersecurity, the effect of fake news, security on the Internet of Things, and the possibility of the use of cyber weapons in different types of conflicts.

These are just some of the discussions that we see emerging in different areas at a global level.

Both the need to increase access to the Internet and these other emerging issues, configure new challenges that cannot be solved with the same political tools and mechanisms with which we faced problems in the past.

New challenges demand new approaches – approaches that are innovative in terms of both content and form.

All these years of building and perfecting Internet governance systems have convinced many of us that the participation of all actors, the search for consensus, and collaborative governance and transparency must be key pillars of these innovative models with which we must deal with new challenges. These governance systems are what we usually refer to as "The Multistakeholder model".

Never before has it been so clear that wisdom and experience in society are highly distributed. It is impossible to think that a single stakeholder (government, civil society, technical community or the private sector) can alone have all the knowledge necessary to design and implement the best solutions.

However, building this new model poses challenges, one being capacity building in all sectors in order to really achieve meaningful participation.

It is important to know the issues and the different policy options in order to deal with each of them. In addition, it is important to know the experiences in other parts of the world, the evaluations of those experiences, and the impacts of different policies in other areas. However, it is also very important to learn that policy development is not a zero-sum game, as collaboration and consensus building generate value for society.

We come from very different traditional models in which building majorities is one of the basic pillars, different from building consensus like in the model we propose. This model change is not trivial

The Internet Governance Schools are fundamental initiatives to build the capacities that are necessary in the construction of successful multistakeholder models of Internet governance.

This book celebrates today the tenth anniversary of the South School on Internet Governance, an initiative that has trained thousands of people who participate today, or even lead debates and policy development, promoting these new models that we need.

Many people who currently hold positions of influence in governments and other sectors in Latin America and the Caribbean have participated in the different editions of the South School on Internet Governance. They had the opportunity not only to learn, but also to acquire the necessary skills to participate actively and constructively in debates at the local, national and regional levels.

For us in the Internet Society, the construction of multistakeholder models of governance is a priority to face concrete problems in a way in which the synthesis of different interests, knowledge and experience allow the development of policies that generate real benefits for people.

Initiatives such as the South School on Internet Governance coincide with those objectives and this is why we share their 10th anniversary with the pride of having supported this initiative all these years and congratulating them for their success.

The success of the South School on Internet Governance is an asset for the region, which together with other successful initiatives, constitutes a solid foundation on which we can continue working for the creation and strengthening of participatory and open Internet governance mechanisms in Latin America and the Caribbean.

This book, which includes important contributions to current issues, is one more step to promote the knowledge generated at the regional level in these matters, to continue to generate critical mass, and to collaborate with the search for the best future for the regional community.

About the Authors

Luca Belli, PhD is Professor of Internet Governance and Regulation at Fundação Getulio Vargas (FGV) Law School, in Rio de Janeiro, where he directs the CyberBRICS project. Luca is also Associate Researcher at the Center for Comparative Public Law at the University Paris 2 Panthéon Assas. Before joining FGV, Luca worked as an agent for the Council of Europe Internet Governance Unit and served as a Network Neutrality Expert for the Council of Europe. Over the past decade, Luca has authored and edited more than 30 research outputs in English, French, Italian, Portuguese and Spanish, amongst which "De la gouvernance à la régulation de l'Internet" (Berger-Levrault, 2016); the "Net Neutrality Compendium" (Springer, 2016); "Platform Regulations: How Platforms are Regulated and How They Regulate Us" (FGV, 2017) and "Gobernanza y Regulaciones de Internet en América Latina" (FGV, 2018) and the "Community Network Manual" (FGV-ITU-ISOC, 2018). Luca's works have been i.a. quoted by the Organization of American States Report on Freedom of Expression and the Internet (2013); used by the CoE to elaborate the Recommendation of the Committee of Ministers on Network Neutrality (2016); featured in the French Telecoms Regulator (ARCEP) Report on the State of the Internet (2018), and published or quoted by various media outlets, including Le Monde, BBC, The Hill, O Globo, El Pais, El Tiempo, La Vanguardia and La Stampa. Luca was the co-organizer of the ninth edition of the South School on Internet Governance, at FGV.

Olga Cavalli co-founded the South School of Internet Governance in 2007 and has been its academic director ever since. The *South School on Internet Governance* is a pioneering program that awards Fellowships to students from Latin America and the Caribbean to receive intensive training in Internet Governance and thus become part of the new leaders of Internet Governance in the region. Between 2007 and 2014, Mrs. Cavalli was a member of the MAG, Multistakeholder Advisory group of the United Nations-Secretary General for the Internet Governance Forum. As an advisor to the Ministry of Foreign Affairs of Argentina, she represented Argentina in the second phase of the WSIS held in Tunisia. She was a member of the Special Commission appointed by the

Government of Argentina to develop the Cyber-Crime Law, and she was a prominent member of the commission that developed the National Digital Agenda of Argentina.Currently in this position, she represents Argentina in the Governmental Adivisor Committee of ICANN, GAC. She is a member of ISOC's global Board of Trustees and was the President of ISOC's Argentine Chapter, ISOC Ar. Since 2012, she is also the Academic Director of DOMINIOS LATINOAMERICA. Mrs. Cavalli has a PHD in Business Direction, an MBA, a Master in Telecommunications Regulation, and she is an Electronics and Electric Engineer.

Carlos Álvarez is Director of Security, Stability and Resilience at ICANN. Currently his work focuses on helping the Internet community to address the abuse of the Domain Name System resources by providing experience on contractual issues and policies with possible implications of anti-abuse and consumer protection. In addition, he promotes trust-based collaboration with cybernetic law enforcement agencies around the world and the safety community, and the creation of capacities through the training of the application of the law and other elements involved in the operation or security of Internet identifiers. He served in the past on the ICANN Contractual Compliance Team, where he managed the team responsible for processing all complaints related to registrars around the world. He also provided expert advice and guidance on the subject in the ICANN Contractual Compliance Audit Program and work related to the gTLD registry compliance team. Prior to joining ICANN, Carlos participated in the International Attorneys Program at Holland & Knight in Miami and served as head of the Division of Legal and Commercial Affairs at Sony Music for Colombia, Ecuador, Venezuela and Peru. Carlos is a lawyer graduated from the University of Los Andes in Bogotá, Colombia. He holds a master's degree from the Gould School of Law of the University of Southern California has a background in TCP / IP networking at UCLA and is a Certified Fraud Examiner.

Pablo Bello Arellano has been Secretary General of ASIET since June 2011. He is an Economist from the University of Chile, with an MBA from ESADE Business School. He has held, among other positions, as Vice-Minister of Telecommunications of the Ministry

of Transport and Telecommunications of Chile, in the Government of Michelle Bachelet. He was also Head of the Regulatory Policy and Studies Division of the Under Secretariat of Telecommunications. He is a leading expert advisor on economic and telecommunications regulation. He was a member of the Global Commission on Internet Governance, the international commission that drafted the report "One Internet", and is currently a member of the Multistakeholder Advisory Group of the Internet Governance Forum.

Horacio Azzolin is a lawyer, graduated from the Universidad Católica Argentina (1996). He did a postgraduate course in criminal law at the Universidad de Palermo (2002), and has more than 25 years of experience in the Argentine justice service. He began his professional development in the Judicial Branch, where he went through all the categories of the judicial career up to the position of Instructing Judge. Since 2008, he has been Federal Prosecutor, specialized in litigation of complex cases related to organized crime and massive human rights violations. From 2013 onwards, he is in charge of cyber-crime, first as the focal point of the National Attorney General's Office and, from the end of 2015, as head of the Specialized Cyber-Crime Prosecutor Unit (UFECI). In addition to representing the organization in various national and international fora, he was appointed Public Prosecutor's Office contact point in the Ibero-American Network of International Legal Cooperation (IberRed), in the specialized network of the Ibero-American Association of Public Prosecutors (CiberRed) and national contact point in the high-tech crime network of the Group of 7 (G7 24/7 Network of High Tech Crime).

Carlos F. Baca-Feldman holds a PhD in Sociology from the Institute of Social Sciences and Humanities Alfonso Vélez Pliego de la BUAP. In this same institution, he developed his Master's studies in Sociology and, previously, the Bachelor's Degree in Communication Sciences by UDLAP.

He has taught at different universities in the city of Puebla and has published several texts on community communication in Mexico. He coordinates the Research Area of REDES A.C.

Filipe Batista is a Graduate in International Relations from the Lusíada University of Lisbon, Post-Graduate in International

Relations from the Institute of Social and Political Sciences and in "Acão Externa da União Europeia", from the Faculty of Law of the University of Lisbon, Master in Development and International Cooperation from the Higher Institute of Economics and Management. He was Deputy Director General of the Cabinet for European and Cooperation International Relations of the Ministry of Justice and Deputy Director General of the Directorate General for Justice Policy of the Ministry of Justice. He is currently Head of the Cooperation and Development Division of ANACOM and Secretary General of the Association of Communications and Telecommunications Regulators of the CPLP (ARCTEL-CPLP), also ensuring the functions of coordinator of the Permanent Secretariat of the Meeting of Ministers of Communications of the CPLP.

Sebastian Bellagamba is currently Director of the Regional Office for Latin America and the Caribbean at the Internet Society. Previously he was President of the Argentine Association of Internet Service Providers, Member, Audit Committee, LACNIC; President, Argentine Chapter, Internet Society Chapter Argentina, IPv6 Task Force. Current Member, Address Supporting Organization Council, ICANN.

Humberto Carrasco Blanc is a lawyer from the Universidad Austral de Chile, LLM in Commercial Law, Universidad del Desarrollo and LLM in Computer and Communications Law from Queen Mary, University of London. He received his doctorate in Law from the University of Edinburgh and is also an associate professor at Universidad Católica del Norte – Chile. He has published several articles in different magazines and publications. In addition, he has participated as a speaker in different conferences. He is also Chair of LAC RALO (Latin American and Caribbean at Large Organization) of ICANN (Internet Corporation for Assigned Names and Numbers). His areas of practice are Corporate Law and Finance, Regulation, Contracts, Licenses, Telecommunications, Competition Law and Intellectual Property.

Adrián Carballo is a co-founder of the South School on Internet Governance and currently the Director of Institutional Relations of the South School of Internet Governance and Director of Marketing and Business Strategy for Latin American Domains. He also serves as Director of CCAT – LAT, High Technology Training Center for

Latin America and the Caribbean, a non-profit organization that is ITU Training Center of Excellence and organizes every year the South School on Internet Governance and Latin American Domains in different countries of the region. He has served as an advisor to UNESCO on connectivity and content projects for rural schools, library digitization and e-commerce projects for the development and integration of rural cooperatives. Previously, he was Coordinator of the MERCOSUR Technology Advisory Committee for Productive Integration at the Subsecretariat for Economic Integration for the Americas and MERCOSUR at the Ministry of Foreign

Affairs of Argentina. Adrián Carballo was also the Coordinator of the Financing Commission of the Regional Action Plan for the Information Society eLAC 2010.

Vinton G. Cerf has served as vice president and lead Internet evangelist at Google since October 2005. From this position, he contributes to the development of global policies and the continuous standardization and promotion of the Internet. He is also an active representative of Google in the Internet world. Cerf is the former senior vice president of Technology Strategy at MCI. In this role, Cerf was responsible for guiding the development of the corporate strategy from a technical perspective. Previously, Cerf served as senior vice president of architecture and technology for MCI, leading a team of architects and engineers to design advanced network schemes that include Internet-based solutions to deliver a combination of data, information, voice and video services to businesses and consumers. Widely known as one of the "Internet Parents", Cerf is a co-designer of the TCP / IP protocols and the Internet architecture. In December 1997, President Clinton presented the United States National Medal of Technology to Cerf and his colleague, Robert E. Kahn, for having founded and developed the Internet. Kahn and Cerf received the Alan M. Turing ACM award in 2004 for their work on Internet protocols. The Turing Prize is also called the "Nobel Prize in Computer Science."

Margarita Valdés Cortés is a lawyer and Legal and Commercial Director of NIC Chile at the University of Chile. She is responsible for the design of administrative and commercial policies as well

as administration of the system of resolution of conflicts of the registration of domain names under.CL. In addition, she has a Master's Degree in Business Management from the Adolfo Ibáñez University Business School. Together with her participation in the Steering Group of NIC Chile and in the National Council of Names and Numbers, she has participated as a guest professor in the Summer School of Intellectual Property organized by WIPO and INAPI and as a guest professor in the Magister program of New Technologies of the Faculty of Law of the same University. Margarita was President of LACTLD (Organization of Administrators of ccTLDs of Latin America and the Caribbean) and participates as advisor of the ccNSO of ICANN (Internet Corporation for Assigned Names and Numbers), where her participation is relevant in the development of Internet policies.

Nadine Andrade Chorão, born in Lisbon, Portugal, is a Graduate in International Relations from the Catholic University, and Master in Business Sciences at the School of Economics and Management. She is an Adviser to the Secretary of ARCTEL-CPLP (Association of Regulators of Information and Telecommunications of the Community of Portuguese Language Countries) since 2012, where she coordinates several development and cooperation projects of the Association ranging from e-commerce training and the universal service. The specialization in the area of development for the communications sector began in 2010 in the Division of Cooperation and Development of the Department of Foreign Affairs of ANACOM, where he developed his functions until joining ARCTEL.

Mark W. Datysgeld holds a bachelor's degree and a Master's degree in International Relations, focusing on Internet governance and the impacts of technology in the formulation of public and private policies. He is affiliated with the business constituency of ICANN, supporting Latin American entrepreneurs in their participation in the institution. He previously attended ICANN meetings as NextGen, NextGen Ambassador, Fellow and Fellow Coach, and participated in IGF as a local staff, workshop organizer and panelist.

Lacier Dias is a Professor and Technical, Regulatory and Academic Director at Sonlintel focusing on process improvement, dissemination of technical knowledge and standardization following the model of

good operating practices focused on routing for Internet access providers, networks and business operators. A member of ICANN's ISPCP, he acts as a national and international conscientized on issues of equipment management for backbone management and control, monitoring, incident prevention and response, expert support, infrastructure, expansion planning, and network engineering.

Danilo Doneda is a Lawyer and Professor at IDP and an advisor to the Brazilian Internet Steering Committee (CGI.br). PhD in Civil Law (UFRJ). Member of the advisory boards of the United Nations Global Pulse Privacy Group, the Project Children and Consumption (Instituto Alana) and Open Knowledge Brasil. Served as General Coordinator at the Ministry of Justice (Brazil). Former visiting researcher at the Italian Data Protection Authority (Rome, Italy), University of Camerino (Camerino, Italy) and at the Max Planck Institute for Comparative and International Private Law (Hamburg, Germany). Authored books, papers, and articles about civil law, digital rights, privacy, and data protection.

Raúl Echeberría joined the Internet Society in 2014 as Vice President of Global Engagement after completing his 6-year term on the Internet Society Board of Directors, of which he was its President for 3 years. Raúl was one of the founders of LACNIC (the Internet Address Registry for Latin America and the Caribbean), where he played a key role in the construction of this Regional Community. He served first as Chairman of the Board and then as Executive Director of LACNIC between 2002 and 2014. He was one of the members of the Working Group on Internet Governance (WGIG) created in 2004 by the Secretary General of the United Nations and played an important role in the negotiations that took place on this issue at the 2005 Summit in Tunis. In 2006 he was again honored by the Secretary-General of the United Nations, being elected to the Multisectoral Advisory Group of the Internet Governance Forum, in which he served until 2014. Raúl is recognized for his participation in the Internet community and for his work in promoting the development of the Internet both regionally and globally. Raúl resides in Uruguay.

Luã Fergus holds a bachelor's degree in Law from Fluminense Federal University (UFF), having participated, in 2016, in the Padre

António Vieira Program at New University of Lisbon (NOVA). He is currently a research assistant at the Center for Technology & Society (CTS) and CyberBRICS Project's Community Manager. He is a founding member of the Youth Special Interest Group of the Internet Society (Youth SIG – ISOC), where he served as Head of the Editorial Committee in the 2015-17 biennium.

Pedro Augusto Francisco is a PhD candidate in Cultural Anthropology at the Federal University of Rio de Janeiro. He holds a master's degree in cultural anthropology and a law degree. He worked as a Project Leader and Researcher at the Center for Technology and Society at the FGV Law School in Rio de Janeiro, from 2009 to 2018. His practice area is the intersection between Anthropology of Science and Technology, Economic Anthropology and Political Anthropology. Currently, his research interests are national security, privacy and surveillance, intellectual property and piracy.

Oscar Robles Garay is the Executive Director of LACNIC, the Internet Address Registry for Latin America and the Caribbean, an international non-governmental organization established in Uruguay and responsible for the allocation and administration of Internet numbering resources for the region. Prior to LACNIC, Oscar worked for 20 years on issues related to domain names NIC México, the organization responsible for .MX Internet domain. He has led various Internet institutions in Latin America and the Caribbean as co-founder of LACTLD – the organization of ccTLDs in Latin America and the Caribbean. He is also a co-founder of LACNIC and one of the promoters of the .LAT Internet domain. Robles has worked with Internet Governance, IP Addresses and Internet Domains since 1995. He has actively participated in the creation of ICANN and various regional Internet-related structures. Oscar Robles graduated as an engineer in computer systems and master's in management of information technology, both from the Tecnológico de Monterrey.

Raquel Gatto is a lawyer and is currently Regional Policy Manager for Latin America and the Caribbean in the Internet Society (ISOC). Prior to this position, she served as director of the Internet Society Brazil Chapter. She is also a member of the Internet Governance Multistakeholder Advisory Group of the United Nations (IGF-MAG).

On the academic side, she holds a doctorate in law focused on Internet governance at PUC-SP. She is also a member of the Global Academic Internet Governance Network – GigaNet -and former Chair of the Program Committee.

Agustín Garzón He is a lawyer with a Master's in Administrative Law from the Austral University (tp). He previously served as Legislator of the City of Buenos Aires, Director of the Buenos Aires Sur Corporation (G.C.B.A.), and Legal Secretary of the Council of the Magistracy of C.A.B.A. and in the General Secretariat of the G.C.B.A. He is currently the Executive Manager of the Ente Nacional de Comunicaciones de Argentina (ENACOM).

Julio César Vega Gómez is the General Director of Internet Association MX, and a lawyer graduated from the Intercontinental University with a Master's Degree in Information Technology and Communications Law at the University of Oslo, Norway. He has been Deputy Director of Electronic Commerce Regulations at the Ministry of Economy, where he worked on issues such as Personal Data Protection and the regulation of unsolicited data messages and maintained a close relationship with the information technology industry.

Jorge Javier Vega Iracelay is an Argentine resident of Mexico with a Law Degree from the Pontificia Universidad Católica Argentina. He also holds a Master of Laws degree from Columbia University (New York), where his thesis on International Arbitration in Investment Disputes was selected for publication. He is a member of the New York State Bar Association. Jorge is currently a University Professor at the Universidad Pan Americana and INFOTEC in Mexico, a researcher, writer and lecturer on topics related to Technology and Society, and collaborator with Nexos Magazine, El Financiero, and other specialized media. In the past, he was Assistant General Counsel of Microsoft Corporation in charge of Legal Direction, Corporate Affairs and Philanthropy at Microsoft Mexico. In 2008, Microsoft Corporation recognized Vega Iracelay with the "Global Attorney Excellence Award". In 2010, he was awarded by the company the "Circle of Excellence" worldwide for its contribution to Corporate Social Responsibility and in 2016 as a member of the General Counsel Power List in Mexico, he was published by The Legal 500. He was Vice Chair of the local chapter of the BSA

(Business Software Alliance), as well as President and Member of the Advisory Council of the Mexican Internet Association and is currently an Advisor to Mamá Digital, a Civil Society organization.

Edison Lanza is the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights since October 2014. He is a Uruguayan lawyer and graduate of the Faculty of Law of the University of the Republic of Uruguay. The Rapporteur has also worked as a journalist in various media, led cases related to the right to freedom of expression before the Inter-American Human Rights System, and integrated, directed and founded several non-governmental organizations defending the right to freedom of expression.

Cláudio Soares Lopes has been a member of the Public Ministry of the State of Rio de Janeiro since 1987. He is a former Attorney General of MPRJ, former president of the National Council of Attorney Generals of the State and Union Public Ministries (CNPG), former professor of the School of Magistracy of the State of Rio de Janeiro (EMERJ) and of the School Foundation of the Public Ministry of the State of Rio de Janeiro (FEMPERJ).

Daniela Parra Hinojosa is a professor of Latin American Studies at UNAM and holds a degree in Communication from the Universidad Iberoamericana Puebla. She teaches at the National School of Higher Studies (ENES) of the UNAM Morelia campus. Since 2006, she has collaborated in popular communication projects in Latin America. For instance, Daniela has researched on alternative communication, Latin American popular integration, among other topics. She coordinates the Dissemination area of REDES A.C.

Maryleana Méndez Jimenez is an engineer with a Master's Degree in Information Technology Management. She has extensive experience in corporate networks, both in the country and abroad. In addition, she has experience in public institutions, such as the Comptroller General of the Republic and in international companies. She worked as project manager for TecApro Internacional (member of the BT Alliance Program) in several Latin American countries.

Peter Knight is an economist specializing in the use of information and communications technologies to accelerate socio-economic

development. Founding member, researcher and member of the Council of the Fernand Braudel World Economics Institute in Sao Paulo and author and/or organizer of seven books on the Internet and development, he has held various technical and management positions at the World Bank, Cornell University, the Ford Foundation, the Brookings Institution and the Training Center for Economic Development (CENDEC). He graduated from Oxford University and Dartmouth University and holds a PhD from Stanford University.

Eduardo Magrani is Coordinator of Law and Technology at ITS Rio, Senior Fellow at the Alexander von Humboldt Institute for Internet and Society, and Research Associate at the Law Schools Global League. He is a PhD student and Master in Constitutional Law from the Pontifical Catholic University of Rio de Janeiro (PUC-Rio). Eduardo is also Visiting Professor of "Law and Technology" and "Intellectual Property" at the Graduation of the Getulio Vargas Foundation Law School and PUC-Rio. E He was a researcher and Project Leader in the areas of E-democracy, Internet of Things and Disruptive Technologies at the Technology Center and Society of FGV, and has been a lawyer since 2010 acting in the fields of Digital Rights, Corporate Law and Intellectual Property. Eduardo is a permanent member of the Commissions of "Law and Information Technology", "Legal Education" and "Legal Aspects of Entrepreneurship and Startups" at OAB-RJ, and author of several books and articles in the area of Technology and Intellectual Property, including: "Connected Democracy" (2014), "Digital Rights: Latin America and the Caribbean" (2017) and "The Internet of Things" (2018).

María Álvarez Malvido holds a degree in Social Anthropology from UAM-Iztapalapa. Her research has focused on the processes followed by various indigenous and community radio stations in Mexico. She has published in media such as Animal Político, Bricolaje, Journal of Students of Social Anthropology and Human Geography, Mi Valedor Magazine and currently collaborates in the section "Culture and daily life" of the digital platform of Nexos Magazine. She coordinates the Indigenous Community Connectivity Project with the support of the Internet Society's Beyond the Net program.

Laura Schertel Mendes is a Professor for Civil Law at the University of Brasília (UnB) and at the Institute for Public Law (IDP), Brazil. She holds a PhD from the Humboldt University of Berlin, Germany, with a thesis about data protection in the private sector, turned into book (Schutz vor Informationsrisiken und Gewährleistung einer gehaltvollen Zustimmung, De Gruyter, 2015). She is the head of the Center for Law, Internet and Society (CEDIS/IDP) and a member of the board of directors of the German-Portuguese Law Association. She worked as a General Coordinator for Market Studies at the National Department for Consumer Protection (Brazilian Ministry of Justice).

Oscar A. Messano is an Argentine citizen, founder and current President of eCom-Lac, the Latin American Federation for Internet and Electronic Commerce, and founder and for many years' president of Lacnic, the Latin American and Caribbean Internet Address Registry. Oscar is also founder and current Secretary of CABASE, the Argentine Chamber of Internet, member of the Board of ISOC-AR Internet Society Argentine Chapter and was Rapporteur on Internet, Ecosystem and International Connectivity in the Advisory Committee of the Inter-American Telecommunications Commission on Telecommunications/ICTL (CCPI CITEL). Oscar is founder and current President of the High Technology Training Center for Latin America and the Caribbean (CCAT-LAT) and specialist of the International Telecommunication Union on Connectivity, Broadband and Traffic Exchange Points. Oscar is also founder and current CEO of Tecnomedia, a company specializing in digital media, videoconferencing and video streaming.

Christian O'Flaherty is Senior Development Manager for Latin America and the Caribbean at the Internet Society. A graduate in Computer Science and Postgraduate in Business Management, he was a teacher, director of operations of the Argentine academic network, regional Internet planning manager at Impsat Fiber Networks and responsible for the Internet product for Latin America at Global Crossing**.**

Renan Medeiros de Oliveira is a researcher at the Center for Justice and Society of the Getúlio Vargas Foundation (CJUS/FGV) and at the Fundamental Rights Clinic of the Faculty of Law of the UERJ – UERJ Rights Clinic. Permanent Researcher of the Laboratory of Economic Regulation of the UERJ – UERJ Reg. Renan has a

Master's Degree in Public Law and a Bachelor's Degree in Law from the University of the State of Rio de Janeiro (UERJ) and a Postgraduate Degree in Public Law from the Pontifical Catholic University of Minas Gerais (PUC Minas).

Eduardo Molina Quiroga is a lawyer born in Mendoza in 1948. He holds a Ph.D. in Civil Law from the University of Buenos Aires, with a thesis rated as outstanding and a recommendation for the Faculty Award. He is a regular adjunct professor of Civil Law (Real Rights) at the Faculty of Law UBA and professor of Postgraduate Studies at UBA and other universities. He co-directs the Career of Specialization in Computer Law (UBA). He is an expert evaluator at CONEAU. He has written more than 10 books, including the Treaty on Computer Law (with Daniel Altmark), and numerous book chapters and publications in legal journals. He is regularly invited to conferences, panels, and round tables on topics of Computer Law. He was amicus curiae before the Argentine Supreme Court in the Rodriguez vs Google case. He directs an UBACyT research project on tensions generated by new technologies applied to video surveillance and the rights to privacy and the protection of personal data. He is Executive Secretary of the Judicial Training Center of the Autonomous City of Buenos Aires and Academic Secretary of the Judicial Training Institute of the Argentine Provinces and C.A.B.A. (Reflect).

Bruno Ramos is the Regional Director of the International Telecommunication Union for the Americas. Bruno is an Electronic Engineer graduated from the Polytechnic School of the University of São Paulo and holds two Master's degrees. One is in Telecommunications Regulation and the other in Electronic Engineering, both from the University of Brasilia (UnB). Engineer Ramos is responsible for the planning, organization and direction of the work of the ITU Regional Office and the coordination with the ITU Area Offices located in Barbados, Chile and Honduras. Mr. Ramos acts directly in the supervision of the activities of the Office, in coordination with the ITU headquarters in Geneva and its team in the region in matters related to international technical cooperation projects implemented in the areas of regulation, administration and monitoring of the radioelectric spectrum, strengthening of telecommunications entities, infrastructure and development of human capacities, among other matters.

Karla Velasco Ramos holds a bachelor's degree in International Relations from ITAM with specialized studies in public policy and macroeconomics from the Institute of Political Studies in Paris (SciencesPo). In 2016 she was chosen as one of the fifteen students for the social entrepreneurship program Innovation for Equality carried out by the University of Berkeley and Prospera, a Mexican non-profit organization. She coordinates the International Area of REDES AC where she focuses on issues of international political advocacy for community networks.

Andrés Sastre has been Regional Director of ASIET for the Southern Cone since 2012. He holds a degree in Law from the Complutense University of Madrid and a Master in Economics from the University of Salamanca. An expert advisor in telecommunications regulation and Internet Governance, he is part of the management of the Internet Governance Forum for Latin America and collaborates within the private sector in the strategy of eLac, the digital agenda for Latin America.

Vanda Scartezini was educated as an electronic engineer specializing in R&D management. Her career spans more than 35 years in managerial positions in the ICT sector, both in the public and private sectors. She advised the government and helped write and implement many fundamental laws throughout Brazilian commercial life, from integrated circuit laws, information technology laws, software, copyright, patents and agricultural varieties, defending them in Mercosur and the WTO. She is currently a partner of two consulting companies in ICT, Internet and intellectual property: POLO Consultores Associados & IT.TREND is also chair of the Board of FITEC, an ICTs research and development center (www.fitec.org.br), and a board member of two other ICTs R&D institutions. From the social area of IT, she is vice president of a local association of women of IT called Nexti and one of the managers of an international group for the empowerment of women: DNS Women group.

Vanessa Fusco Nogueira Simões is a Promoter of Justice of the State of Minas Gerais, Brazil. A Graduate in Law from the Federal University of the State of Minas Gerais, she completed her Doctorate in Law at the University of Barcelona in 2011. She taught at the Center for Studies, Criminality, and Public Security of UFMG, teaching the

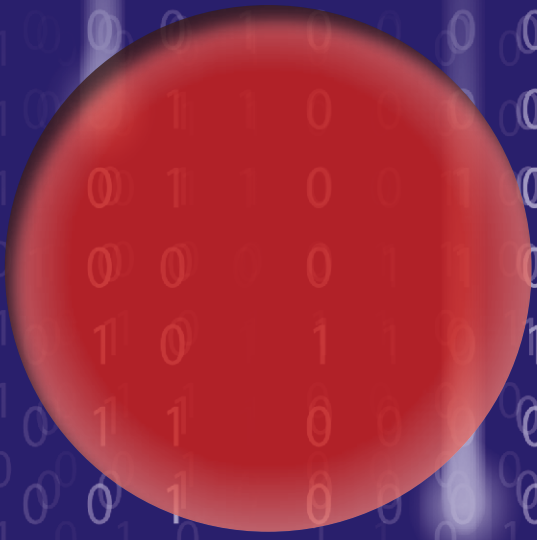
discipline of Law and Social Control. She was responsible for the creation of the first Public Prosecutor's Office to Combat Cyber Crimes in Brazil in 2008. She is a member of the Committee to Confront Trafficking in Persons of the State of Minas Gerais.

Hugo Fusco Nogueira Simões is a lawyer specializing in cyber-crimes. He acted as an intern in the Public Ministry of the State of Minas Gerais. He studied American Law at the University of Minnesota, USA, and has a post-graduate degree in Criminal Sciences from FUMEC University, in Belo Horizonte.

Christoph Steck is Director of Public Policy and the Internet at Telefónica. He directs advocacy and defines its positions on Internet Policy and Governance and other policy issues that shape the Digital Economy. He is Vice-President of the BIAC Digital Economy Policy Committee (OECD) and of the Digital Economy Commission of the International Chamber of Commerce (ICC), Co-President of OMAC of the Internet Society (ISOC) and President of the International Affairs and Internet Governance group of ETNO (the European Telecommunications Association). In addition, he represents Telefónica in various international organisations (such as G20, ITU, and ICANN) and is a recognised expert and speaker on digital policies. He has directed the publication of Telefónica's widely recognized and influential Digital Manifesto. Christoph studied law at the Universities of Cologne, Munich and London (UCL) and is a qualified German lawyer with a Master's degree in Business Administration (MBA) from IE University where he is also an Associate Professor.

Erick Huerta Velázquez has a PhD in Rural Development from UAM Xochimilco, a Master in Social Administration with a specialization in Community Development from the University of Queensland, Australia, and a Law Degree from the Universidad Iberoamericana with postgraduate courses at the Escuela Libre de Derecho. He is an expert of the International Telecommunication Union (ITU) for connectivity issues in remote areas and indigenous people. He designed the legal strategy of the first Indigenous Community Cell Phone Network in the world. He is the Deputy General Coordinator of REDES A.C.

INTRODUCTORY SECTION



1 Ten Years of the *South School on Internet Governance*

Olga Cavalli*, *Adrián Carballo* and *Oscar Messano

One of the unique characteristics of the Internet is the way in which its creators, based on a distributed global coordination of its resources, conceived it. There is no single place of control, no president and no small group of officials who govern it. The Internet works thanks to millions of independent networks, with different owners, with different technologies, distributed all over the world, coordinated thanks to the work of organizations that elaborate rules and protocols so that they work together, giving us the incredible experience of a single global network.

Given its particular governance, it is clear that the analysis of its rules and standards, its impact on the economy, on society and on daily life, is a source of great interest for a wide range of actors.

The World Summit on the Information Society documents includes a definition of Internet Governance that shows the intrinsic essence of the multiple stakeholders involved in its functioning:

> "Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet[2]."

There is a variety of spaces for participation and debate where these "principles, norms, rules and procedures" are defined, which constitues the global coordination of the Internet and where the different interested parties or *stakeholders* interact: ICANN, IETF, IGF, LACIGF, LACNIC, meetings of the ITU International Telecommunications Union, among other national, regional and global meetings.

Although these meetings are generally open to the community, it is not easy to participate actively from the beginning. The topics

2 See <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html>.

reviewed are complex and the dynamics of each meeting are different. It takes some time to get actively engaged in dialogue.

Fellows and experts of SSIG 2014 organized in Port of Spain, Trinidad and Tobago.

How can the region take its relevant issues to these debate spaces? How is it possible to enhance the participation of our representatives in an active and effective way? How can we help our young representatives to get involved in the Internet Governance ecosystem? How can we train the future Internet Governance leaders from our region?

The South School on Internet Governance was created to help the community to answer these questions with concrete actions. Since its creation, the objectives of the South School on Internet Governance are the following:

- Create a learning space for new generations of professionals who actively participate in meetings where the future of the Internet is shaped.
- Help training the new leaders on Internet Governance in each of the region´s countries.
- Consolidate a relevant regional representation in meetings and fora where the Internet Governance is debated and defined.

Opening of South School on Internet Governance in Bogota, Colombia, in 2012.

There are several barriers to achieve an active and relevant participation of our regional community, one of which is the language. It is for this reason that *South School on Internet Governance* has offered in all its editions English – Spanish simultaneous translation and in the two editions organized in Brazil simultaneous translation English – Spanish – Portuguese. Simultaneous translation allows both experts and fellows to easily interact, promoting anactive participation during the activity program.

The South School on Internet Governance rotates among countries in the region; it is organized each year in a different country. This rotation allows for a greater involvement of each of the communities in which it is organized. It also allows participants from other countries in the region and faculty members to interact with the local community where the school is organized.

The South School on Internet Governance has been organized with great success in the following countries:

- Buenos Aires, Argentina (March 2009)
- Sao Paulo, Brazil (March 2010)
- Mexico City, Mexico (April 2011)
- Bogotá, Colombia (March 2012)
- Panama, Panama (April 2013)
- Port of Spain, Trinidad and Tobago (April 2014)
- San Jose of Costa Rica, Costa Rica (April 2015)
- Washington DC, OAS Headquarters (Organization of American States), USA (April 2016)
- Rio de Janeiro, Getulio Vargas Foundation, Brazil (April 2017)
- CYBER SSIG Washington DC, OAS Headquarters (Organization of American States), USA (April 2018)

In order to promote the training of professionals who wish to gain skills on Internet Governance, in order to become actively involved in the Internet ecosystem, the South School on Internet Governance offers fellowships to all its participants since its first edition. The fellowship includes the course, study materials, hotel accommodation and meals. For fellows who live close to the venue or wish to stay on their own, fellowships are available without hotel accommodation.

Group of fellows of the South School on Internet Governance 2017 at the headquarters of the Getulio Vargas Foundation in Rio de Janeiro, Brazil, 2017.

The selection of fellows is made jointly with the host institution after a broad call for participation, which is disseminated through social networks and various virtual media. The group of fellowship holders selected based on:

- The greatest geographical diversity
- Gender balance
- The greatest diversity in *stakeholder* representation and professional background and experience
- There is no age limit

Since its fourth edition organized in Bogotá, Colombia (2012), the South School on Internet Governance in addition to the face-to-face activities, also offers remote participation open to the entire community through video streaming and audio in two or three channels (Spanish and English, and in Brazil, Spanish, English and Portuguese).

Vint Cerf, father of the Internet with the founders of the *South School on Internet Governance*, Olga Cavalli and Adrián Carballo before their participation in the South School on Internet Governance 2016 at the headquarters of the Organization of American States OAS in Washington DC, in 2016.

Since 2012, remote participation has increased year by year. The largest remote participation was registered in 2016 during the eighth edition organized in Washington DC, at the OAS Headquarters (Organization of American States), with 25,000 remote participants from 89 countries during the five days of activity.

It is important to emphasize the role of each host organization, which is fundamental in convening the local community, playing an important role in the organizational and logistical development of the entire event, and in allowing the contact with local experts who will be part of the faculty.

A special mention deserves the support of a large number of governments, companies, and organizations that every year contribute with the fellowship program to organize the South School on Internet Governance.

Each edition of the South School on Internet Governance has the participation of the most recognized Internet experts in America and Europe, all of them recognized personalities related to Internet Governance, who interact with the group of fellows during the five days of the activity.

The South School on Internet Governance generates also new spontaneous initiatives among the participants. Each year the organization creates an e-mail and a Telegram group for the group of fellows, and they spontaneously generate other information exchange groups on Facebook, Twitter, and WhatsApp. All these means of communication continue to be used by each group of scholars who, after the school, keep in touch, exchanging useful information for their work, working opportunities, social activities and many other information.

SSIG 2016 organized at the OAS headquarters in Washington DC, honored with the presence of Vint Cerf, father of the Internet, in the center of the photo.

In 2016, at the initiative of the ISOC Barbados Chapter, a remote hub was organized locally in a university classroom with the participation of 60 fellows who followed all the five day´s activities and were able to ask questions remotely.

In the ten editions of the South School on Internet Governance, more than 2300 scholarship holders have been trained in person and thousands more remotely. Dozens of experts from all over the world have participated as lecturers. Many of the fellows today are deeply involved holding relevant roles in organizations, governments and businesses related to Internet Governance.

The ten years of South School on Internet Governance represent a wonderful journey through our beautiful region, in contact with groups of fellows who are interested in the impact of technology on society and through the permanent evolution of technology and the Internet that each year confronts us with new challenges.

In our role of founders of this wonderful space, we consider ourselves privileged because we have been allowed to create and nurture it over the years. We express our deep gratitude to those who contribute to this initiative, to the host organizations in each country, to all the experts who have contributed with their knowledge and time to enrich the program of activities, to the scholars and remote participants and to all those who in one way or another have collaborated so that the South School on Internet Governance celebrates its ten years of a successful trajectory.

We invite you to travel with us many more years in this wonderful journey of learning and friendship.

Olga Cavalli, Adrián Carballo **and** ***Oscar Messano,***
https://www.gobernanzainternet.org

2 Internet Governance and Regulation: A Critical Presentation

Luca Belli

Since its commercialization and democratization in the 1990s, the Internet has become an integral part of the lives of all connected individuals and an essential tool for the formation of our opinions and to enable us to learn, communicate, socialize, have access to public services and do business, spreading the fruits of our creativity online. Today, the Internet and Information and Communication Technologies (ICT) are increasingly ubiquitous and inexorably linked to our daily activities, relating to our democratic, economic and social lives. An increasingly higher portion of the opportunities we can capture during the course of our lives depends on the possibility of accessing the Internet, while the possibility of avoiding an increasing amount of risks depends on our ability to understand how the Internet works and how we can use it safely, productively and sustainably.

In this context, it should be noted that, if information is the oxygen of the modern age, then the Internet could be considered as the respiratory apparatus of contemporary humanity, which needs to be cared for in a sustainable fashion in order to safeguard a healthy and robust constitution and avoid the evolutions that could prejudge our common well-being.

Thus, the forms of governance and regulation of such a powerful medium, so essential to our lives, have already ceased to be issues limited to specialists and have become subjects debated daily by the public and influenced by a continuous flow of legislative proposals as well as by the decisions of private actors, whose economic dimensions may exceed those of the vast majority of existing states. The digital environment can be seen as the natural environment that surrounds us, where the decisions of public authorities and companies in one specific place can determine positive and negative externalities for all the components of the ecosystem. In the digital environment, the decisions of public and private actors can deploy their effects well beyond the borders of specific countries and well beyond the users of specific products and services.

The recognition of the complexity of the Internet and the interdependence of its elements is the starting point of this book, which does not attempt to exhaustively analyze the evolution and impact of the Internet in the Americas, but rather to offer the necessary elements to understand and question several of the facets that make up the prism of Internet governance and to critically analyze several of the regulatory tools that influence its evolution in the region. Only by understanding the existence, interconnection and, frequently, the contraposition of particular interests and regulatory instruments that shape the evolution of the Internet, will the reader be able to understand the usefulness of governance processes open to the participation of the various stakeholders[3,4] that elaborate and implement the sectoral regulations that define the present and future of the Internet.

Thus, this work adopts a multistakeholder approach in the sense of including a series of very heterogeneous analyses, written by some of the most renowned specialists in the region, from the academic world, the public and private sectors, civil society, and the technical community. This book is particularly relevant not only because it celebrates ten years of multistakeholder debates within the South School on Internet Governance (SSIG), but also because it is the only work in the region that proves with facts and concrete content the usefulness of multistakeholder analysis to know and ponder with attention the variety of points of view and interests that are at stake each time an aspect of the Internet is considered.

The greatest wealth of any multistakeholder exercise is or, at least, should be – the heterogeneity of opinions presented and debated. Only the confrontation of different opinions and the careful analysis of the interests involved can lead to informed decision-making and sustainable approaches. In this sense, examining this book, the reader may find varied and, sometimes, divergent opinions, because the objective of this work is not to offer definitive

3 For a discussion in this regard, see Belli (2016: 312-323).

4 The English term stakeholder defines any natural or legal person involved in the deliberative and decision-making processes that take place at the international, national or local level. The participation of the stakeholders is justified by their interest or "*stake*" In a certain process. In this paper, we will consider the term interest as "the economic or political motivation, or the moral value, that awakens the attention of an individual or an organization in a process, which leads to investment of specific resources to influence the outcome of the process." See Belli (2015).

solutions, but only to communicate ideas and elements of pluralist reflection, to help each one to form his or her opinion in a critical and independent way.

2.1 Substantive questions and Byzantine questions

According to paragraph 34 of the Tunis Agenda for the Information Society, adopted during the second phase of the World Summit on the Information Society (commonly known as WSIS), "Internet governance is the development and application by governments, the private sector and civil society, in the performance of their respective roles, of principles, norms, rules, decision-making procedures and common programs that shape the evolution and use of the Internet".

Although not notable for its precision, this working definition has the considerable merit of avoiding epistemological conflicts over what can be defined as governance[5]. However, the lack of a clarification of how the cooperation of different stakeholders should be concretely implemented leaves the door open for more than a decade of speculation on what can be defined as a multistakeholder process and, above all, what can be a truly open, inclusive or democratic form of multistakeholderism. In this context, since the development of WSIS many – perhaps too many – works in the area of Internet governance have been devoted to the analysis of processes and institutions categorized as multistakeholder and, particularly, to the multistakeholder governance model developed in the field of the Domain Name System (DNS).

Without wishing to diminish the academic interest in debating the different versions and flavours of the various multistakeholder models[6], it seems essential to emphasize that, since attention is a

5 Since the 1980s, the concept of governance has become widespread and the versatility of its use has suggested the existence of almost as many governance concepts as researchers in the field. In contrast to the term "government", which characterizes the governing institution, the term "governance" is generally used to refer to the procedural aspect and, particularly, to the way of governing a system. This concept has been used since the middle Ages to describe the political system characterized by the institutionalized participation of different corporate groups such as the Church, economic actors and territorial powers. Since the middle Ages, many versions of the concept of governance have been elaborated and promoted. See Belli (2016: 35-96).

6 With regard to Internet governance, both the benefits and the risks associated with multistakeholder processes seem particularly tangible. See, for example, Kleinwächter (2007); Hill (2015); Belli (2016).

limited resource, the excessive concentration of such a resource on the analysis of the best form of multistakeholderism has the consequence, *ad minima*, of diverting attention from other issues that have a much greater direct impact on the life of each individual. In this perspective, much attention, specialist efforts and many economic resources have been devoted to relatively marginal elements with comparatively limited impact on the well-being of individuals, such as the definition of an appropriate multistakeholder model for the Supervision of the "IANA Functions"[7] of the DNS. This concentration of resources on such topic can be considered as a non-optimal utilization of attention, efforts and money of a very large community that could have directed their resources towards resolving issues that are much more relevant to Internet users and non-users.

Unfortunately, the perhaps excessive concentration of attention on these latter issues did not allow – or, at least, did not help – to find durable solutions to issues of paramount importance to individuals such as bridging digital divides, protecting privacy and cybersecurity, and establishing competitive national digital ecosystems to harness and disseminate the benefits of technological transformations.

Although the definition of solid multistakeholder processes is very important, the risk of an excessive concentration on formal and procedural issues, instead of concentrating on the various and urgent substantial issues, is a modern reproduction of the famous debate on the sex of angels, known to be the Byzantine question par excellence.

According to legend, during the Turkish invasion of Byzantium in 1453, politicians, bureaucrats, notables and philosophers, together with all inhabitants of the city, failed to realize the magnitude of what was happening at the gates of the city, because they were all engaged in the endless discussion about the sex of angels. Thus, as the Byzantines did not consider and respond adequately to the most important challenges, already at their doorstep, they ended

7 It is in this sense that we can point out that the cost of the transition project of the IANA Functions – a project that was announced in March 2014, before the conference known as NETmundial, a conference convened in reaction to the so-called "Snowden revelations" – was approximately USD 34 Million. See <https://www.icann.org/resources/pages/iana-transition-project-cost>.

up being colonized by the Ottomans and, by the way, they did not even manage to define what the sex of the angels could finally be.

In such a perspective, the objective of the organization of this book was not to concentrate the efforts of the different authors to debate the details of the best possible model of multistakeholder governance, but to use the indisputable competences of the specialists selected for this publication to offer analyses with different and stimulating perspectives, sometimes even provocative, on some of the issues that we consider to be the most important for the digital future of the region and that, thirteen years after the WSIS, remain unresolved.

The issues discussed in this book are at the heart of the governance processes and regulatory efforts that are defining the advancement of the Internet and demonstrate that our ability to develop and enjoy fundamental rights is considerably influenced in relation to how the Internet and ICTs will develop in the region. The importance of this point is enormous and represents the guiding thread of the whole book, being carefully analyzed in its different perspectives by the contributions of the authors. The opportunities and challenges that the Internet, its governance and regulations are facing in the region are masterfully explored, starting from the prefaces of Vint Cerf, one of the fathers of the Internet, and Raúl Echeberría, Vice President of Global Engagement of the Internet Society, to the conclusions of Edison Lanza, Special Rapporteur for Freedom of Expression of the Organization of American States. Throughout the four parts of this book, the reader will be led to explore the evolutions and gaps of the Internet infrastructure in the region, to ponder the measures likely to promote a sustainable expansion of connectivity, to analyze the challenges of privacy and cybersecurity, and finally to consider a selection of technological, regulatory and social transformations that the region is called upon to face.

2.2 Multistakeholder governance and regulatory instruments

When considering naturally complex and multifaceted issues, it is necessary to analyze carefully the political, legal, economic and social consequences that certain decisions may have. Thus, the complexity,

technical sophistication and inevitable social impact of the Internet highlight the interest of the approach chosen for this publication, offering a broad spectrum of expert opinions to promote informed debates and support the elaboration of policies and regulations, based on empirical data and on diverse points of view.

In this perspective, the use of the term governance in reference to the Internet seeks to frame the mechanisms that favor the interaction and association of the different stakeholders in a political space where divergent ideologies and economic interests are confronted. Therefore, Internet governance can be considered as the set of processes that should stimulate the comparison of ideas and, ideally, promote the collaborative formation of new "international regimes"[8] that allow the smooth functioning of the Internet.

On the contrary, the different regulatory instruments are the product of these governance processes that can be more or less participatory. The objective of regulation is to foster equilibrium and ensure the proper functioning of complex systems[9], within which a plurality of independent actors interact in a disorderly manner, animated by divergent purposes and interests. In light of this consideration, it is important to note that the different tools that regulate the Internet may be of public origin, such as international conventions, laws, regulations and decisions made by national courts and agencies, but may also be private in nature. In the latter case, private regulation may be contractual, such as the terms and conditions[10] defining the rules for the use of web platforms[11], mobile applications and Internet access networks, or technical, such as the algorithms, standards and protocols defining the software and hardware architectures that determine what users can and cannot do in the digital environment[12].

8 One of the least known cases of plagiarism in the world of Internet governance is the very definition of Internet governance that is "freely inspired" by the famous definition of international regime elaborated by Stephen Krasner, according to which the regimes are sets of "Implicit or explicit principles, norms, rules and decision-making procedures around which the expectations of the actors in a determined area of international relations converge." See Krasner (1983).

9 Frison-Roche (2002:314).

10 In this sense, see the study "Terms of Service and Human Rights", developed by the Technology and Society Center of the Getulio Vargas Foundation, in association with the Council of Europe, available at <http://tinyurl.com/toshr>.

11 For an analysis on the regulation of digital platforms, see Belli and Zingales (2017).

12 See Reidenberg (1998); Lessig (2006); DeNardis (2009); Belli (2016).

The normative dynamics that arise between the regulatory instruments mentioned above highlight the benefits of a multistakeholder approach not only to confront the ideas of different stakeholders but also to stimulate the compatibility of the various regulatory instruments that can be developed by such stakeholders. Thus, in the digital ecosystem, the normativity does not only origin within the state. On the contrary, the most prevalent – and most effective – forms of regulation are those of a private nature, which we can define as "lex electronica," or contractual agreements, and as "lex informatica," or the software and hardware that define the architecture of the internet[13]. In this context of normative pluralism, the collaboration of diverse stakeholders becomes instrumental in order to stimulate the elaboration and implementation of efficient and sustainable regulatory strategies, considering all the externalities – positive or negative – that one type of technology or one type of regulation can deploy on affecting the interests of all stakeholders.

In continuity with the multistakeholder approach promoted by the SSIG over the last ten years, this book brought together a series of particularly valuable analyses that, not only can be used to inform the readers, but also represent an excellent basis of discussion for the promotion of sustainable policies and regulations. Thus, the contributions included in this volume seem particularly useful, first, to identify the various aspects of different digital problems that are common to the countries of the region and, second, to identify alternative solutions to the regulatory approaches that have already been experimented to date and which, in many cases, have shown to have limits or to be simply ineffective.

The different contributions included in the four parts of this book are presented briefly in the following sections.

13 The formulas *lex electronica* Y *lex informatics* intentionally approach the expression *lex mercatoria*, to highlight its origins and developments outside traditional political institutions. Thus, *lex mercatoria* refers to the set of rules that were developed and implemented by medieval traders to regulate cross-border trade in the absence of an effective state authority. See Belli (2016: 133).

2.3 Infrastructure between evolutions and gaps

The first part of this volume is dedicated to providing a panorama of digital infrastructure in the region, critically analyzing the evolutions and challenges that are being faced by different stakeholders. This part is opened by Bruno Ramos' analysis of the transforming function of Internet infrastructure, in his chapter dedicated to "**Invisible Communications: Social Inclusion and Development through Telecommunications/ICT**". Ramos argues that, when one examines our time, it can be observed that behind a superficial image of great transformation, the social foundations of the late twentieth century continue to exist without major changes, both from the economic point of view of supremacy between nations and the separation between the most and least favored classes. However, within the field of study of telecommunications and ICTs, technological transformations are driving a remarkable evolution in the way people interact, changing the way they observe physical and social space. Communications serve as a driving force for transformation through access to information, being everywhere, as an invisible being that guides us towards new horizons, making it possible to reduce differences and include vulnerable people.

Thus, the author explains that in order for this mechanism of inclusion and development by telecommunications and ICTs to become an engine of social welfare, it is necessary to establish an environment favorable to the flowering of these "invisible communications", including the construction of a governance model that allows their growth, following broader and wider principles of action, and the implementation of infrastructure for the flow of information in areas with a high volume of traffic and in the most remote areas without investment. In conclusion, Ramos discusses the problems that exist against the establishment of this environment of inclusive invisible communications and the various courses of action that can be traced to combat them, keeping alive the possibility of new disruptive visions.

Ramos' analysis is perfectly complemented by Maryleana Mendez Jimenez's chapter on "**The Fundamental Role of Telecommunications Infrastructure**," where the author argues that telecommunications

infrastructure has been, is and will be the cornerstone on which the entire digital ecosystem rests. Therefore, its goal in the 21st century is to bring a robust, fast and secure Internet to the largest number of people, which results in the public benefit of a more connected society and the private benefit of a stronger market. The author emphasizes that the technological advance, as well as the search for efficiency in the provision of the service, have generated changes in the scope, scale, ownership and amortization of this infrastructure. In a hyper connected world, the productive and intensive use of technology will determine the survival of business and the stability and growth of the economy as a whole.

The telecommunications industry has evolved to make its processes more efficient and thus be able to support the strong and necessary investments in maintenance and infrastructure development, despite being the only component of the highly regulated digital ecosystem. Regulatory frameworks and regulators must be adapted and consolidated in order to remain relevant in the new economic environment, and change must begin now.

The role of the regulator must evolve into a promoter of the investment needed for the digital economy, as well as being watchful of healthy competition and emphasizing the protection of the end user, especially in terms of security and privacy.

In his chapter on "**The Challenges of Internet Access**" Oscar Robles Garay reminds us that the unconnected represent 50% of the planet's population and that this percentage includes the most vulnerable groups and geographically isolated areas, which poses a greater challenge than connecting the first half of the population over the last 30 years. However, this cannot be an excuse to ignore the challenges that exist with regard to those already connected, challenges that also establish evolving and growing objectives in the coming years, which require an Internet which is well suited to face the current challenges and able to stay open. Based on this reflection, the author explores the challenges that are present in any economy, not only for the least developed countries, highlighting the importance of keeping them in our discussions with the aim of establishing sustainable solutions.

Subsequently, Agustín Garzón explores "**The evolution of telecommunications: technology, public policies and regulation in Argentina**" highlighting how the progress of telecommunications has generated a dynamic development of ICT Services and applications, capable of generating considerable opportunities. Among these services, not only traditional services such as telephony and broadcasting stand out, but also new digital services, that lead to the analysis of current issues such as Regional Digital Market, Artificial Intelligence, Industry 4.0, Cybersecurity and 5G, among others. Likewise, the author indicates that the development of telecommunications has tended toward technological convergence, allowing the provision of different services through the same infrastructure, which requires an appropriate regulatory framework that favors and encourages the development of the sector allowing users to access a greater range of services, in an affordable manner and in equitable social and geographical conditions.

In order to achieve the above-mentioned objectives and generate a suitable environment for the implementation of telecommunications and ICTs services, an adequate telecommunications infrastructure is indispensable and that is why public policies focus on the deployment of infrastructure. In this perspective, Garzón details the main technological trends as well as the regulatory tools that favor their implementation, while describing the main difficulties faced by the sector and the regulatory measures and public policies developed to resolve them.

The Argentine context is explored differently by Oscar Messano, in his chapter on "**National and International Connectivity: the Case of the IXP Buenos Aires**". Based on his professional and personal experience, the author recounts a journey in the Argentine connectivity, which includes a little more than 30 IXP and whose participants are of varied national and international origin, such as NGOs, SMEs, governments, academics, incumbent companies, business leaders, among others, making the IXP Buenos Aires an interesting laboratory for the gestation and performance of "multiple stakeholders." Highlighting the existence of challenges, Messano discusses how to overcome these difficulties is part of any innovative activity. The author explores the success case of the IXP

Buenos Aires, highlighting how today the project "Federalization of broadband" is in full growth and produces a permanent exchange of information with the IXPs in the region. This experience has led to the creation of LAC-IX "Association of Internet Exchange Points in Latin America and the Caribbean", a non-profit organization based in Uruguay, which brings together several countries with IXPs in the region: Argentina, Brazil, Caribbean, Colombia, Costa Rica, Cuba, Ecuador and Paraguay.

In his chapter on "**The Technological Evolution of Internet Pathways**", Lacier Dias explores Internet access in Latin America and the Caribbean, addressing the growing need to be connected, the impact that access has on the digital economy, and the lack of legal security for entrepreneurs and users who still persist in the region.

To address these topics, the author begins with the historical trajectory of the types of physical infrastructure, routing protocols, and data routing technologies used in connectivity. In addition, Dias presents some perspectives for a future scenario, dealing with the implementation of Internet Protocol version 6 (IPv6), the growth of community networks and the important role played by small and medium providers. Finally, the article deals with the geographical, social and economic barriers faced by people dedicated to providing access to the network in the most diverse locations not covered by large commercial providers.

Subsequently, Peter Knight presents an X-ray of the state of broadband Internet in Brazil, in his chapter on "**Broadband Infrastructure and Digital Inclusion in Brazil**", analyzing the evolution of its penetration from 2006 to 2016 (i.e. digital inclusion) and offering a comparison of this penetration and the prices of fixed and mobile broadband with other countries. The author also discusses the quality of broadband service and explores some factors that affect the price of broadband in Brazil, highlighting mainly the extremely high taxation that impacts the entire telecommunications sector, but also the degree of competition, the high costs of financing and installing networks and leasing infrastructure from other operators, and the low public sector investment in networks.

Knight then analyzes federal public broadband policies in Brazil, with emphasis on the development of the National Education and Research Network (RNP), the privatization of telecommunications since 1998, and the National Broadband Plan. The author highlights the lack of effective priority of federal and state governments in relation to broadband expansion and digital inclusion and, finally, presents some conclusions on the importance of holistic strategic planning to take advantage of ICTs and their analogical complements to accelerate economic, social and political development of the country; the evolution of broadband in Brazil compared to other countries; and the federal government's programs for broadband expansion and digital inclusion.

Finally, the first part of this book ends with Luca Belli's analysis of "**Network Neutrality, Zero Rating and the *Marco Civil da Internet***". The evolution of the debate on net neutrality is explored starting from an international perspective, reaching the Brazilian case and analysing the compatibility of the net neutrality includes with the practice of sponsoring access to specific applications, called *zero rating*. Discussions on these issues have intensified considerably in recent years, covering the whole of Latin America, and more specifically Brazil, which recently passed law 12.965, known as the *Marco Civil da Internet*, and its regulation, decree 8.771 of 2016, which have addressed the protection of several fundamental rights in the online environment and have regulated net neutrality in Brazil.

The practices of Internet traffic discrimination, the diffusion of so-called *zero rating* models and, consequently, the discussions on the principle of non-discrimination called network neutrality have taken on considerable proportions in the region. This popularization of the net neutrality debate is due to the awareness of an increasing number of individuals that the possibility of having access to the Internet in a non-discriminatory manner directly impacts their ability to enjoy their fundamental rights: communicating, innovating and conducting businesses freely online. After an analysis of network neutrality, the author offers a critical exposition of *zero rating* practices and analyzes how these issues are regulated by the Marco Civil da internet. Finally, he explores the potential negative effects of these practices and mentions future ways to address access issues in a sustainable manner.

2.4 A sustainable expansion of connectivity

The second part of this book explores ideas, proposals and strategies that can and should be discussed to overcome existing connectivity gaps, projecting the countries of the region towards a sustainable and inclusive digital future where everyone can reap the benefits of connectivity.

In this perspective, in the first chapter of this second part Luca Belli analyses the importance of "**Community Networks and the Principle of Network Self-determination**". The author argues that any individual should enjoy the right to "network self-determination" and that such a principle, although not yet recognized *de jure*, is already being implemented *de facto*, thanks to the development of community networks. Community networks are collaborative networks and are established in a *bottom-up* fashion by members of local communities who develop and manage the network infrastructure as a common good. The principle of network self-determination, as far as it is concerned, must be considered as the right to freely associate in order to define, in a democratic way, the design, development and management of the digital infrastructure, in order to freely seek, transmit and receive information and innovation.

Belli argues that the principle of network self-determination finds its conceptual basis in the fundamental right to self-determination of individuals, as well as in the principle of informational self-determination, on which data protection is traditionally grounded. The author emphasizes that network self-determination plays a fundamental role, allowing individuals to associate and join efforts to bridge digital divides in a collaborative manner. In this perspective, this chapter examines a selection of community networks, highlighting the positive externalities of such initiatives that favor the establishment of new participatory governance structures and the development of new content, applications and services that address the needs of local communities, empowering previously disconnected individuals. The analysis offers evidence that the development of community networks can induce various benefits, creating learning opportunities, stimulating

local entrepreneurship, promoting the creation of new jobs and reinvigorating social connections in communities, through multistakeholder partnerships that bring local institutions closer to entrepreneurs and community members.

The discussion about the potential and importance of community networks continues with the analysis of Christian O'Flaherty on the "**Building Community Infrastructure: Technologies and Disruptive Models**". The author, taking as a backdrop the strategic interests of the Internet Society in promoting community initiatives, aims to demonstrate how the future of the Internet and sustainable connectivity should use the principles of collaboration and cooperation to reach the underserved regions by commercial providers of Internet access. To do this, the work uses various practical examples already existing to explain succinctly the functioning of community networks, addressing their characteristics and the challenges they face for the expansion of that model. In dealing with technical and regulatory barriers to the application of community networks, the article lists a number of obstacles, such as legislation, permits and licenses that relate to spectrum management and the use of public infrastructure, and also indicates the need to develop a wide range of materials that are suitable for alternative networks, from the construction of equipment, through the development of standards and protocols, and the training of equipment to operate this entire system. Finally, reiterating the theme of the Internet Society, this work highlights the need for disruptive models of governance and sustainability for community networks, models that will be fundamental to achieve the goal of making the Internet everyone's.

In "**Re-think Public Policies to Close the Digital Divide in Latin America**", Pablo Bello and Andrés Sastre highlight that Latin America has made significant progress in recent years in terms of connectivity, but there are still significant challenges to achieve the closing of the digital divide and the full insertion of the region in the Information Society. The authors emphasize that understanding the transformations that have taken place in the digital ecosystem in recent years, particularly the phenomenon of convergence, and the factors that influence the decision-making processes regarding

investments in networks, is fundamental for public policies to promote the configuration of virtuous circles of competition, innovation and greater coverage of connectivity services.

Recognizing the remarkable advances of recent years allows us to assess those factors that have helped to democratize access, but at the same time it highlights the magnitude of the pending task and confirms that the path that remains to be traveled is more complicated than the already travelled.

Bello and Sastre argue that, in order for Latin America to start an economic growth that can reduce poverty and generate opportunities for progress and equality, it is essential to increase productivity and transform the structure of value creation. That is why the digitalization of production processes is one of the most important economic policies that we have to carry out. Achieving the closing of the digital divide and having a world-class connectivity infrastructure is a necessary, though not sufficient, condition for moving in that direction.

In his chapter on "**A New Model to Increase the Infrastructure of Access and Use of the Internet for a Digital and Inclusive Society**," Christoph Steck stresses that the availability of broadband infrastructure is one of the first requirements for people to access the Internet and enjoy digital services such as banking or access to online health services. It is also important for the development of companies, since digitization is fundamental for their operation and competitiveness. On the other hand, the author recalls that there is a part of the population that even having access to infrastructure, does not connect, so it is necessary to address both problems in an aligned manner, with the help of both public and private sector, each one in the exercise of their powers. Thus, the private sector must innovate in technology and in business models in a way that allows it to make infrastructure sustainable in areas where it is not today. In this sense, the public sector should focus all its actions on allowing that sustainability to occur, and that the regulations allow us to face this challenge with guarantees.

Steck points out that the private sector must find new business models for Internet access, both as regards offers to users and

better exploiting the double-sided market natire of the Internet, so that not all the economic effort falls exclusively on consumers, but on the entire value chain of digital services.

The author argues that the public sector should be concerned about digital training of the population so that it is able to take advantage of the content and services offered. In addition, they should avoid using ICTs services as a direct source of income, since the economic impact on society of investments in the ICTs sector is greater due to the competitiveness factor that it adds. Steck affirms that we are facing a digital revolution that is transforming society in a way and at a never seen speed and it is the responsibility of the public sector and the private sector to make this process inclusive, leaving no one, on the margin.

An example of how alternative solutions of sustainable connectivity can be implemented concretely is offered by Filipe Batista and Nadine Chorão in their chapter dedicated to "**Expansion of Infrastructure and Internet Access: The Experience of the *Sustainable Villages for Development***". In this work, the authors present the project *Sustainable Villages for Development* (SV4D), designed to promote digital inclusion and designed taking into account the heterogeneous characteristics of the countries of the Community of Portuguese Language Countries (CPLP) and prepared by the Association of Regulators of Communications and Telecommunications of the Community of Countries of Language Portuguese (ARCTEL-CPLP) together with the Research and Development Association – Fraunhofer. The authors highlight that the central idea of the SV4D project is to create a network of laboratories focused on the research and development of ICTs solutions for development. These solutions should meet the needs of developing countries with particular regard to the mission of ARCTEL – CPLP, which is the development and universalization of communications services in places where major sector deficiencies are present. Batista and Chorão describe how this objective can be achieved, creating the necessary conditions for the promotion of development and local training.

In this perspective, SV4D stimulates the expansion of connectivity and offers the students of the technological areas the possibility of

developing their ideas in the laboratories dedicated to the project, with the support of the teams of ARCTEL-CPLP and Fraunhofer.

Finally, this second part is concluded with a chapter that not only gives us concrete evidence on how community networks can be built, but also gives us valuable instructions on how to do so. In "**Weaving Technological Autonomy in Indigenous Peoples: Community Cellular Telephony in Oaxaca, Mexico**", Carlos F. Baca-Feldman, Erick Huerta Velázquez, María Álvarez Malvido, Daniela Parra Hinojosa and Karla Velasco Ramos explore the example of Oaxaca's indigenous communities in Mexico. Since 2013, these communities have started a revolutionary use of the radio spectrum, giving rise to the first community cellular telephony networks in the world, which has triggered a process that disrupts the traditional organizational forms of telecommunications. The authors analyze this process highlighting that it was possible thanks to the collaboration of native communities and hackers, supported by two social organizations Rhizomatica and REDES A.C. Later, in 2016, the emergence of the AC Indigenous Community Telecommunications organization allowed the consolidation of a project in which, for the first time, the communities themselves own and operate their own community networks that offer mobile telephony services.

The authors argue that the particularity of this innovative experience lies in the legal, technological, economic and organizational bases of a model based on the notion of the spectrum as a common good and that is capable of considerably helping to connect to the next billion in a sustainable manner. Thus, this chapter describes and analyzes the characteristics of this experiment, in conjunction with its contextual dimensions, to understand the possibilities, limits and contradictions of this form of technological appropriation.

2.5 The challenges of privacy and cybersecurity

The third part of this book is dedicated to two topics that, unfortunately, are frequently explored separately, namely privacy and online security, with a particular focus on the regulations on the protection and use of users' personal data.

This part begins with Danilo Doneda and Laura Schertel Mendes chapter providing "**A Profile of the New Brazilian General Data Protection Law**". The authors analyze the importance of the new General Data Protection Law (LGPD – Law 13.709 / 2018) to guarantee the rights of Brazilians in the 21st century, highlighting how the approval of the law consolidated a normative framework for the information society, complementing and dialoguing with other norms defined by the Brazilian legal system. The chapter analyzes the main axes of LGPD, with particular emphasis on principles and rights contained in the new law. Finally, it examines the main challenges for the implementation of LGPD in the country.

Subsequently, Eduardo Molina Quiroga's chapter on "**Privacy, Personal Data and Tensions with Online Freedom of Expression**" emphasizes that the right to privacy, or to private life is protected by international Human Rights laws and principles established in the second half of the 20th century, is related to the right to the protection of personal data, without prejudice to the conceptual autonomy that this right has reached in the last three years of the last century. Quiroga argues that both concepts undergo a notable change with the spread of ICTs and especially the Internet. The conflict unleashed in this scenario pits these rights against other freedoms, such as freedom of expression. In this context, the author attempts to describe the main characteristics of the aforementioned rights and to present a proposal of criteria to be taken into account when resolving such conflicts.

Subsequently, in "**Big Data is Us: New Technologies and Personal Data Management**" Eduardo Magrani and Renan Medeiros de Oliveira present a critical vision about the use of personal data in the current hyper connectivity scenario, bringing to the surface, as an alternative, the possibility of self-management of data, based on a specific project. The authors present, first of all, a panorama of privacy in the 21st century, highlighting that it is a multifaceted right that has gained new contours in the face of contemporary technologies and that has challenges still unanswered. Second, Magrani and Oliveira explore the notion of Big Data, a term that

describes any voluminous amount of structured, semi-structured or unstructured data that has the potential to be exploited to obtain information.

The authors highlight the idea that Big Data is us and that we have incentives to regain control over this information. Lastly, they analyze the personal data management project called MyData, which in Latin America is currently promoted only in Brazil, by the Center for Technology and Society of the Getulio Vargas Foundation. The authors conclude the analysis with the defense that a project of this type can be an effective alternative to protect the right to privacy in the contemporary world.

In his chapter on "**Mi casa es su casa: The Impact of Digital Assistants on Privacy in Latin America**", Luã Fergus Oliveira da Cruz studies the impact and potential threats that digital assistants can bring to Latin American users and consumers. At first, Fergus develops his analysis through a bibliographic research on the recent implications regarding the privacy provided by these products and applications, analyzing literature on the use of Big Data in the Global South. Subsequently, the author develops a an abnalysis analysis of patent applications, terms of use and privacy policies of the Alexa assistant, which are generally used by the Echo family devices, both developed by the Amazon Company, currently the main player in the market. The study makes a forecast for a scenario in which such assistants are increasingly present in households in the region and, finally, aims to protect the privacy of users of these devices.

Cláudio Soares Lopes explores **the** "**Right to Be Forgotten in Brazilian Justice in the Era of the Fake News**", noting that the constant growth of the number of Brazilians connected to the Internet, the proximity of the 2018 elections and the emergence of the debate about the so-called fake news, are converging with the debate on the right to be forgotten and its possible interpretations before the Brazilian Justice. Taking into account the dictatorial past and the recent Brazilian democracy, and through the analysis of the current Brazilian legal system, the recent decisions issued by the high courts and the best doctrinal understandings, the author presents the different interpretations

existing on the recognition of the right to be forgotten, presenting which ways and solutions could be followed in the next trials of the Supreme Federal Court of Brazil.

The Brazilian context is explored from another perspective by Vanessa Fusco N. Simões and Hugo Fusco N. Simões, in their chapter on "**Challenges in Obtaining Evidence in Cybercrimes in Brazil: The WhatsApp case**". The authors highlight that the Brazilian population is increasingly using the Internet, both through *smartphones* and computers. The authors emphasize that the increase in digital inclusion seen in the last ten years in Brazil, mainly through the mobile Internet and to access social networks, also brings the migration of criminals to the virtual world. However, the Brazilian criminal and procedural legislation did not accompany the speed of Internet access, and research and the establishment of a criminal action against cybercrime is currently an arduous task for the operators of the Criminal Justice system. In this perspective, the authors argue that doctrine and jurisprudence, technicians and lawyers debate the phenomenon of cybercrime but still do not find effective solutions. More and more crimes occur with impunity in the virtual environment in Brazil and the application of legislation can become particularly arduous, as the WhatsApp case demonstrates.

Reflecting on cybersecurity, Carlos S. Álvarez explores the question of "**Who is Responsible for Internet Security?**" The author comes to the conclusion that Internet security is a matter for everyone. However, what does this really mean? When everyone is involved, it becomes easy to dilute personal responsibility to make it almost disappear? Adopting a critical and multifaceted approach, Álvarez provides elements of analysis in relation to the roles that correspond to the different actors and sectors in society and refers to the responsibilities that are expected to be honestly accepted and assumed voluntarily by each actor in the society.

In short, this third part is concluded by Horacio Azzolin with his reflection on "**The Legal Framework for Cybercrime**". The author states that the appearance of the first cyber-crimes allowed us to notice that most Latin American countries were not sufficiently prepared to face the phenomenon of cybercrime.

Over time, the professionals involved have learned that the investigation of these cases requires states to prepare in several aspects. The adoption of a national cybersecurity strategy, the establishment of response centers for cyber-incidents, the sustainability over time of prevention campaigns aimed at citizenship and the maintenance of properly equipped and trained police forces are some of them. Azzolin suggests that an issue that, for various reasons, is sometimes left out is the issue of the normative system. In this sense, the author evokes the need for substantive laws, which define crimes, and in order to establish rules of procedure, as well as international cooperation mechanisms. The author proposes to review what are the most important aspects that policy makers should take into account when reviewing the legislative system of their countries.

2.6 Technological, regulatory and social transformations

The fourth part of this book analyses some examples of the technological, regulatory and social evolutions that are transforming the region and that will probably shape our digital future.

These transformations are first explored by Luca Belli, Pedro Augusto Francisco and Nicolo Zingales, in "**Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police**", where the three authors argue that digital platforms are increasingly undertaking regulatory and police functions, which are traditionally considered a matter of public law. The authors emphasise that such functions have been growingly delegated to platforms by public authorities, while at the same time platforms are self attributing such functions to avoid liability, de facto becoming private cyber-regulators and cyber-police.

After highlighting the tendency towards delegation of public functions to private platforms, we provide concrete examples of such phenomenon. For example, the chapter illustrates three types of delegations of public power: the imposition of openended injunctions against innocent intermediaries, typically for content removal or website blocking; the implementation of the right to content delisting against search engines, also known as the "right to be forgotten"; and the enlisting of numerous IT companies into a voluntary scheme to counter "illegal hate speech". We show in all these cases that the

amount of discretion conferred on platforms is problematic from the standpoint of the protection of individual rights.

Furthermore, the paper scrutinises the case of the parallel copyright regime developed by YouTube, to emphasise another collateral effect of the privatisation of regulation and police functions: the extraterritorial application of a national legislation – US copyright, in this case – which de facto turns the platform into a private proxy for global application of national regulation. We conclude highlighting some of the challenges and viable solutions for the protection of individual rights in an era of increasing privatisation of regulation and police.

Subsequently, Sebastian Bellagamba and Raquel Gatto offer an overview of how we are "**Building the Future of the Internet with our Youth Voices**". Bellagamba and Gatto present the challenges and opportunities that users, communities and societies will face in the immediate future, basing their considerations on the *Paths to Our Digital Future* report, launched in 2017 by the Internet Society. This analysis was based on forecasts about the future of the Internet taken from a wide range of sectors, and among the set of recommendations derived from the contributions received — the authors focus on one of them, which seems particularly crucial: the training and empowerment of young people. This issue, which has been gaining more and more space in digital policy discussions, is addressed through an analysis of documents and statements dealing with the participation of digital natives, and points to the need to raise awareness among youth and get them actively involved in Internet Governance processes.

Next, Vanda Scartezini analyzes "**Disruptive Technologies and their Impacts in Latin America**", stressing that technological evolutions are responsible for the most important evolutions in humanity since time immemorial and that the main developmental revolutions were all linked to the disruptive technologies of their time. Based on one of the most relevant technologies present today in our day-to-day life – the Internet – the author discusses new technologies technologies that she argues will impact, to a greater or lesser extent, the future of the Latin American societies. It is about the exploitation of what will or will not be relevant in

the near future. Scartezini argues that discussions on these issues are taking place in various forums around the world and explores a subset of interest within the context of Internet Governance. In particular, the author raises some points of relevance to our region, such as a platform for discussions and alerts for our governments regarding measures that need to be put into practice to guarantee the development of our nations and the economic and social future of the new generations.

In his chapter devoted to the "**Regulatory Perspective of Artificial Intelligence**", Jorge J. Vega Iracelay addresses the growing development of artificial intelligence applications and solutions, asserting that this evolution brings with it many questions about how this phenomenon will impact our lives, our interaction with machines and computers. Within these questions, the possibility of regulating artificial intelligence and its interaction with human beings themselves is the most relevant. In this context, Vega-Iracelay points out some of the challenges posed by artificial intelligence and suggests certain regulatory parameters to address them eventually from the legal perspective.

Subsequently, Julio César Vega Gomez analyzes "**E-commerce in Mexico**", emphasizing that the adoption of the Internet during the last 20 years in Mexico is a reality that today is especially tangible through online transactions. E-commerce has evolved by leaps and bounds and more and more companies from different industries, including traditional ones, see online commerce as a sales channel option. Companies of all sizes have begun their path in the adoption of e-commerce. Consumer confidence, although it still has areas of opportunity, is favorable to electronic transactions and the market invites everyday companies from various countries to join the Mexican market. However, Vega Gomez argues that, notwithstanding the foregoing, several threats today come from the regulatory trench. Thus, the author points out that attempts to regulate the Internet and, in particular, to regulate electronic commerce, are often not based on a fair view between consumer protection and business development but, rather and in many cases, on an unclear view of the functioning of this innovative sales channel and the flats and particularities it entails. In this context, the author regrets that this happens at the same time that public

policies fail to have an even stronger ecosystem and avoid a possible commercial digital divide.

Margarita Valdés Cortés and Humberto Carrasco Blanc allow us to explore an innovative system of legal support in "**Leveling the Playing Field: Legal Assistance to .cl Domain Name Holders:**" The authors emphasize that the widespread use of the Internet and its resources has caused domain name users to face a problem that is often unknown to them, such as conflicts over domain names. In particular, natural persons, generally far from these subjects, faced with a controversy, do not understand, do not act or defend their rights, in the context of a domain name arbitration. These dynamics are analyzed in the context of the electronic dispute resolution system for high level domains for Chile, .cl. Valdés Cortés and Carrasco look for a way to create an accompaniment space without cost for users, mostly natural persons, to defend their rights and at the same time, creating an instance of academic learning of electronic litigation in the .cl system.

Thus, the authors describe the collaboration between NIC Chile and the Legal Clinic Chair of the Faculty of Legal and Social Sciences of the Universidad Católica Del Norte.

The experience described in this chapter shows, in general terms, how users can defend their rights and interests and how the dynamics of lawsuits and the quality of arbitral awards have changed when the holder of a .cl domain is legally advised. In addition, the authors argue that the Chilean Internet community reports a distributed social benefit, consisting of free legal defense for its controversies under.cl.

Finally, this part concludes with Mark W. Datysgeld's chapter on "**A Synthesized Connected Existence: How the Internet Could Allow 3D printing to improve the Developing World**". The author explains that while transformative technologies such as Artificial Intelligence have attracted much attention from academia and the media over the years, the subtler development of additive manufacturing has not yet been recognized as an important factor in shaping our future. This chapter examines how the combination of an ever-expanding Internet with increased availability of 3D printers can

provide opportunities for improvement for the developing world. After reflecting on the paradox of globalization that leads to raw materials being sent all over the world only to return as finished products, the author proceeds to make his observations based on empirical research and analysis of technology that is already beyond the proof-of-concept stage, looking at examples from the construction, health and food sectors. With this data in hand, the author's research moves toward understanding the intersection between the consequences of larger-scale 3D printing, a global communications network, and intellectual property rights.

Datysgeld outlines some possible policy pathways for turning the progress of 3D printing into benefits for the developing world, while taking into consideration issues such as job relocation. The author's conclusion is that before the world is taken by surprise by additive manufacturing and policies are promulgated in a reactive manner, it is the responsibility of the actors involved in the relevant arenas to advance a meaningful discussion on the subject, while there is still time for the conformation of a more sustainable logic for our productive system.

2.7 Conclusion

The conclusion of this book has been entrusted to the pen of Edison Lanza, who in his excellent postface dedicated to "**The principles that guarantee a free, open and inclusive Internet for all individuals and social groups**" analyzes the evolution of the protection of freedom of expression and human rights on the Internet in international law. The author emphasizes that the digital environment has enabled citizens to express themselves freely and openly, offers excellent conditions for innovation and the exercise of other fundamental rights such as free association, the right to culture and education. However, the online environment has become increasingly complex in terms of challenges to the exercise of these rights and the free flow of information, including the privacy of individuals. In addition to the problems related to equitable and universal access to the Internet, in recent years there have been other problems related to the legal regime of intermediaries, who support the existence of public space and much of the operation of the network; the challenge

of maintaining the neutrality of the network with respect to content and applications; and the phenomenon of storing and handling huge amounts of personal data on the network, for purposes of security or online surveillance.

In this final text, Lanza seeks to systematize some of the responses and visions from a human rights perspective, with emphasis on the inter-American legal framework. This final vision highlights, in a pragmatic and eloquent way, the principles that are to the basis of a humane and sustainable digital environment, without forgetting the challenges that are analyzed throughout the book.

With a solid argumentation and a rigorous style, Lanza offers us a lucid thought on the elements that we must promote if we want to continue enjoying a free Internet.

2.8 References

Belli, L. (2015). A heterostakeholder cooperation for sustainable internet policymaking. Internet Policy Review, 4(2). <https://policyreview.info/node/364/pdf>.

Belli, L. (2016). De la gouvernance à la regulation de l'Internet. Paris: Berger-Levrault,

Belli, L. y Zingales, N. (Eds.) (2017). Platform regulations: how platforms are regulated and how they regulate us. Official Outcome of the UN IGF Dynamic Coalition on Platform Responsibility. Rio de Janeiro. FGV Direito Rio. <http://bibliotecadigital.fgv.br/dspace/handle/10438/19402>.

DeNardis, L. (2009). Protocol Politics: The Globalization of Internet Governance. Cambridge: The MIT Press.

Frison-Roche, M.-A. (2002). Le droit, source et forme de régulation mondiale. in Jacquet, P., Pisani-Ferry J. y Tubiana, L. (2002). Gouvernance mondiale. Rapport de synthèse. p. 314 <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/024000230.pdf>.

Hill, R. (2015). The true stakes of internet governance. In Buxton, N & Bélanger Dumontier, M. (Eds.) State of Power (2015). An annual anthology on global power and resistance. The Transnational Institute. <http://www.tni.org/sites/www.tni.org/files/download/03_tni_state-of-power-2015_the_true_stakes_of_internet_governance.pdf>.

Kleinwächter, W. (Ed.) (2007). The Power of Ideas: Internet Governance in a Global Multi- Stakeholder Environment. Berlin: Marketing fur Deutschland GmbH.

Krasner, S. D. (Ed.) (1983). International Regimes. Ithaca: Cornell University Press.

Lessig, L. (2006). Code and Other Laws of Cyberspace. Version 2.0. New York: Basic Books.

Reidenberg, J. R. (1998). Lex Informatica: The Formulation of Information Policy Rules Through Technology. *Texas Law Review*. Vol. 76. N° 3.

INFRASTRUCTURE BETWEEN EVOLUTIONS AND GAPS

3 Invisible Communications: Social Inclusion and Development through Telecommunications / ICTs

Bruno Ramos

Note: Please note that the views expressed in this document are those of the author and do not necessarily reflect those of the International Telecommunication Union (ITU).

Abstract

When an analysis is made of our time, in particular the years 2015 to 2030, the period of implementation of the Sustainable Development Goals – SDGs, which were signed by the Member States of the United Nations as a set of guiding goals of the efforts of inclusion and sustainable development, it can be observed that behind a superficial image of great transformation, or a label of "a time of rapid transformations", the social bases of the end of the twentieth century continue to exist without great changes. This is observable both from the point of view of economic supremacy between nations and the inequality between the most and least favored classes. However, within our field of study, namely telecommunications and information and communication technologies (ICTs), technological transformations drive a great change in the way people interact, transforming the way they relate to and observe the physical and social space. Communications serve as a driving force for transformation through ubiquitous access to information. In a sense, it is an invisible being that guides us towards new horizons, enabling the reduction of differences and the inclusion of vulnerable people. Thus, for this mechanism of inclusion and development by telecommunications/ICTs to become a propelling force of social welfare, it is necessary to establish a favorable environment to cultivate these "invisible communications", including the construction of a governance model that allows their growth following broader principles and through the implementation of data flow infrastructure at high traffic areas and remote and neglected regions.

In conclusion, this paper deals with the the barriers that the establishment of this invisible and inclusive communications

environment faces and the various paths that may be traced in order to overcome them, safeguarding the possibility for new disruptive visions.

3.1 Is it time for Transformation? Yes or no? Where are we?

In order for us to be able to address social inclusion and development through telecommunications/ICT[14][15], especially how communications work invisibly as a substrate for the achievement of those goals, we must enter into a sequence of thoughts that passes from where we are now, to where we want to go, and how we can achieve this goal. This is how this article is structured.

In attempting to answer the question in the title of this chapter, we should determine in which field of intellectual, technological, economic or social development, among many others, this analysis of an "epoch of transformation" will be made. From the economic and social point of view, including the intellectual and developmental question of human "wisdom", we are still in a stage close to the last decades of the twentieth century. The economic and influence overlap between nations changes in a morose and moderate way, with sporadic cases of development such as China, but remains generally unchanged. Social differences and economic and social inclusion continue to be unresolved issues by humanity, so much that in the establishment of the Sustainable Development Goals[16], humanity still faces the same problems of

14 Telecommunications: Any transmission, emission or reception of signs, signals, writings, images, sounds or information of any nature by wire, radio, optical or other electromagnetic systems. (Constitution of the International Telecommunication Union, CS / An 1012).

15 ICT (information and communication technologies): A set of equipment, protocols, mechanisms and processes that allow organizing, processing and sharing information and content produced of any nature. (Definition of the Author).

16 In September 2015, more than 150 Heads of State and Government met at the historic Sustainable Development Summit in which they adopted the 2030 Agenda. This Agenda contains 17 universally applicable objectives that, from January 1, 2016, govern the efforts of the countries to achieve a sustainable world in the year 2030. The Sustainable Development Goals (SDGs) are heirs of the Millennium Development Goals (MDGs) and seek to expand the successes achieved with them, as well as achieve those goals that were not achieved. These new objectives present the uniqueness of urging all countries, whether rich, poor or middle-income, to adopt measures to promote prosperity while protecting the planet. They recognize that efforts to end poverty must go hand in hand with strategies that support economic growth and address a range of social needs, including education, health, and social protection and employment opportunities, while combating climate change and promoting environmental protection. The exhaustive list of SDGs is found in <http://www.undp.org/content/undp/en/home/sustainable development-goals.html>. Goal 1: No Poverty; Goal 2:

several decades ago, such as the promotion of inclusive economic growth; promotion and defense of human rights; prevention of conflicts and maintenance of peace among peoples; promotion of justice and international law; prevention of the spread of drug trafficking; protection of the environment and promotion of health and strength for all. However, when we position ourselves and analyze our era from the point of view of telecommunications/ information and communication technologies (ICTs), we notice a characteristic of substantial alteration in the way people interact and in their access to information, although in some cases the communication of information is plain and without substance. Perhaps the main driving force behind this alteration in interactions between people is access to knowledge and education, which allows us to reflect on the stage where we are compared to others, being the driving force for changes, what they are, but adherent to the desires of the people, the result of a clear vision of the world where we live and where we want to go.

Even considering that the principles of electronic engineering and telecommunications remain the same, such as: Boolean algebra, the basis of computational calculations, Maxwell's laws, with the principles that establish the basis of electromagnetism, and Shannon-Hartley's theorem, with the definition of the maximum rate at which information can be transmitted through a communication channel of a certain bandwidth in the presence of noise, which continues to define research in the sense of new techniques of data compression and cryptography, the new technological formulas promoted in particular the miniaturization of users' telecommunications equipment, battery autonomy and video display offers, bringing, with these possibilities, a profound impact on society: the transformation of the way of communicating collectively for the individual.

Zero Hunger; Goal 3: Good Health and well-being; Goal 4: Quality education; Goal 5: Gender equality; Goal 6: Clean water and sanitation; Goal 7: Affordable and clean energy; Goal 8: Decent work and economic growth; Goal 9: Industry, innovation and infrastructure; Goal 10: Reduced inequalities; Goal 11: Sustainable cities and communities; Goal 12: Responsible consumption and production; Goal 13: Climate action; Goal 14: Life below water; Goal 15: Life on land; Goal 16: Peace, justice and strong institutions; Goal 17: Partnerships for the goals.

Thus, although in today's world a certain stability is maintained in the social and economic base and in the historical control relationship, ICTs have been introducing a wedge of transformation, sometimes dichotomous[17], causing individuals to become stronger and, with it, to relate in a more inclusive society, with respect to individualities and to life as a whole.

In theory, this process is a game where individual characteristics, structured by access to information and by the construction of objectives inherent in the feeling of "making a difference", lead each person to have influence over another insofar as the behavior of the first person generates a change in the behavior of the others[18].

Moscovici states that (Moscovici, 1985), (...) "most social objects are ambiguous and that is what distinguishes them from physical objects. We lack clear and precise criteria for judging them". Thus, we have no criteria for assessing truth or error in terms of political or religious opinions, cultural values and norms, and symbols in general. Faced with such objects, individuals may fall to uncertainty, not knowing what precise judgment to make about them.

However, they need one. In order to reduce this uncertainty, some rely on the judgment of others and form a common norm that decides, arbitrarily, what is true or false. This standard is supposed to represent reality. As a result, the norm established in common acquires the force of law for each individual. Each individual no longer sees things through their own eyes, but through the eyes of the group.

In that sense, in Moscovici's view, society, or social groups tend to adjust by exerting mutual influence among their members, seeking to achieve their objectives.

ICTs, especially due to their characteristic of promoting access to information and education (in a comprehensive understanding of their contribution to a more inclusive society), have been

17 Dichotomy: in the Platonic dialectic, partition of a concept into two others, in general, contrary and complementary (for example, human beings: men and women). With respect to the ICTs dichotomy, it can be said that, on the one hand, there is the existence of connectivity making possible a more participatory / democratic social organization, but on the other there is also the possibility of social control, surveillance and manipulation of information.

18 However, we can also mention the existence of an additional perspective such as the social control of third parties over individuals connected through ICT. See Marx (2015) and Lyon (2009).

playing this role of adjustment[19] which allows overcoming fear and appropriation of one's way of thinking, understanding the facts of reality and the manifestation of one's liberty, creating the conditions for the sought-after and notable "transformation" in current times.

3.2 Internet and principles

Since it was conceived as a form of interaction between academic entities, the Internet has been the disruptive "mechanism" for the training of individuals and the basis for the development of this form of individual interaction and, consequently, for social improvement.

By acting as "application layer"[20], or in other words "the content" – including the particularities, inconsistencies and social desires – that is processed, transformed and transported by the electromagnetic telecommunications networks, the Internet is used as the building factor of the "transformation" model towards an inclusive and sustainable society.

Within this prism of application, it is important to form an idea of how to mount a virtuous cycle that allows individuals to train and create the basis for change.

The Internet Steering Committee in Brazil – CGI.br, after intense open discussion with the most diverse social actors, approved, at its 3rd ordinary meeting in 2009, Resolution CGI.br/RES/2009/003/P (CGI, 2009) with the principles for Internet governance, which was subsequently presented in the most relevant international forums, being even presented and internalized by the International Telecommunications Union – ITU as a reference document for the discussions among the diverse international agents on how to build an inclusive, egalitarian, human and sustainable social process.

19 Once again, we can mention the perspective regarding the risks of society online, how the use of ICTs for surveillance, social control, maximization of private interests of few dominant agents as opposed to the interest of the community.

20 The application layer is a term used in computer networks to designate an abstraction layer that encompasses protocols that perform end-to-end communication between applications. In the OSI Model, it's the seventh layer. It is responsible for providing services for applications to separate the existence of communication in network between processes of different computers. It is also layer five of the TCP / IP Model that covers the presentation and session layers in the OSI Model.

These principles are:

1st Freedom, privacy and human rights: The use of the Internet must be driven by the principles of freedom of expression, individual privacy and the respect for human rights, recognizing them as essential to the preservation of a fair and democratic society.

2nd Internet governance must be exercised in a transparent, multilateral and democratic manner, with the participation of the various sectors of society, thereby preserving and encouraging its character as a collective creation.

3rd Universality: Internet access must be universal so that it becomes a tool for human and social development, thereby contributing to the formation of an inclusive and nondiscriminatory society, for the benefit of all.

4th Diversity: Cultural diversity must be respected and preserved and its expression must be stimulated, without the imposition of beliefs, customs or values.

5th Innovation: Internet governance must promote the continuous development and widespread dissemination of new technologies and models for access and use.

6th Network Neutrality: Filtering or traffic privileges must meet ethical and technical criteria only, excluding any political, commercial, religious and cultural factors or any other form of discrimination or preferential treatment.

7th Non-liability of the network: All action taken against illicit activity on the network must be aimed at those directly responsible for such activities, and not at the means of access and transport, always upholding the fundamental principles of freedom, privacy and the respect for human rights.

8th Functionality, security and stability: The stability, security and overall functionality of the network must be actively preserved through the adoption of technical measures that are consistent with international standards and encourage the adoption of best practices.

9th Standardization and interoperability: The Internet must be based on open standards that facilitate interoperability and enable all to participate in its development.

10th Legal and regulatory environment: The legal and regulatory environments must preserve the dynamics of the Internet as a space for collaboration.

Through these principles, the establishment of an environment conducive to the development of favorable conditions for the objectives of inclusion and sustainability is sought.

The SDGs are the goals for the construction of public policies of the Member States of the United Nations, in search of that transformation of inclusion and sustainability, according to Filomena Siqueira, advisor of International Relations of the Educational Action[21]. In order for the SDGs to be integrated into policies there must be clear and accessible monitoring instruments. In the words of the advisor, "through the set of goals, which enables a broad and deep view of the current challenges, the SDGs have the role of strengthening development actions based on three dimensions: economic growth, social inclusion and environmental protection".

To this end, it is necessary to work, both at the governmental level and between civil society and the private sector, on the methodological aspects of Agenda 2030, which involve transparent and disaggregated statistical instruments covering the entire national territory, and the political and operational aspects, which demand commitment from the government in terms of human and financial resources, and monitoring mechanisms that allow for an independent and transparent evaluation, with communication and periodic dissemination of the progress of the agenda".

The Internet and its principles, being implemented and followed, enable the participation of all individuals in this construction and transformation of the world in which we live. Indivdual participation, through the knowledge and education that are made possible by digital "applications", already brings with itself the self-sustainability and monitoring mechanisms that are essential for the continuity of the process of achieving the SDGs in 2030.

21 The Educational Action is a non-profit civil association founded in 1994. Its mission is to promote educational, cultural and youth rights, taking into account social justice, participatory democracy and sustainable development. It carries out training and support activities for groups of educators, young people and cultural agents. It integrates campaigns and other collective actions aimed at realizing these rights, at the local, national and international levels. It develops research, disseminates information and analyzes focusing on public policies in the perspective of human rights and ethnic-racial and gender equality. See <http://acaoeducativa.org.br/>.

3.3 Infrastructure and access

What would be the main problem, or one of the main ones, for the developing countries to reach the situation of "capacity" for the advance in this decrease of the differences of opportunities, in greater inclusion and sustainability?

According to ITU studies (see references on the *MIS Report* – Information Society Measurement Report), as well as the definitions of its Member States, the current stage of the provision of infrastructure for access to the telecommunications network is situated as one of the main issues to be faced by developing countries on the way to establishing the essential conditions for giving people the "capacity" to use Internet applications.

According to the interim final report of the ITU World Telecommunication Development Conference 2017 – WTDC-17, held in Buenos Aires in October 2017 (ITU, Interim Final Report. World Telecommunication Development Conference 2017 – WTDC-17, Buenos Aires, 9-20 October 2017, 2017), "Infrastructure is essential in enabling universal, sustainable, ubiquitous and affordable access to services and ICTs for all. The ICT sector is characterized by the rapid evolution of technology and by the convergence of technological platforms for telecommunications, information distribution, broadcasting and information technology, which are fundamental facilitators of the digital economy. The installation of broadband technologies, including fixed and mobile, and common network infrastructures for multiple telecommunications services and applications, as well as the evolution towards future wireless and wired IP-based networks and their future evolutions, will not only mean opportunities but also important challenges for developing countries. When we refer to communications, we include communications between people, between people and things, and between things, as well as new or emerging technologies".

In addition, it was stated that "broadband is fundamental to the transformation of the traditional economy into a digital economy. The introduction of various broadband technologies will further increase the need for high-capacity broadband and connectivity. Therefore, it is important to provide developing countries

with an understanding of the different available broadband technologies, both wired and wireless for terrestrial and satellite telecommunications, including IMT especially for IMT-2020 and also to support them for applications and services of IoT".

In the WTDC-17 documents, "deployment of broadband infrastructure, especially in rural and underserved areas, and strengthening access to broadband services and applications" was identified as a priority, with "assistance to Member States in identifying needs and developing policies, mechanisms and regulatory initiatives to reduce the digital divide by increasing broadband access and adoption as a way to achieve SDGs".

Without access to the network the inclusion mechanism is broken. Without access to information, an essential part of the use of Internet applications, people in developing countries are not allowed to benefit from basic tools for the flowering of ideas and the implementation of the SDGs, i.e., its objectives of inclusion and sustainability.

This positions telecommunications in a level of essentiality, with all the legal and social discussions inherent in that definition.

As we are dealing with telecommunications / ICT, the focus of the analysis of social transformations will be on this issue. Of course, in the implementation of a more inclusive and sustainable society, as well as in the achievement of the goals of the SDGs, other aspects must be considered, as stipulated in the SDGs themselves, such as the fight against poverty and hunger, ensuring a healthy life and promoting well-being for all ages, ensuring an inclusive, equitable and quality education, achieving gender equality, ensuring the availability and sustainable management of water, ensuring access to affordable, safe, sustainable and modern energy, among others.

Thus, as described above, in order to create the conditions for people to be able to use the Internet tools as a mechanism for individual and, consequently, social transformation, the existence of infrastructure for access to telecommunication networks is a basic element[22].

22 It should be stressed that the existence of infrastructure is a necessary but not sufficient condition for sustainable development. Policies to promote access to infrastructure must be combined with digital literacy policies to promote sustainable development and the participation of connected individuals. This will be elaborated further in Chapter 4 – Invisible communications: with ubiquity, accessibility, human training and reasonable prices.

And how can the economic conditions be formed to encourage and enable the investment and construction of access networks?

In its *MIS Report* – Information Society Measurement Report 2017, Volume 1 (ITU, MIS Report – Information Society Measurement Report 2017, Volume 1, 2017), ITU argues that there is a substantial gap between countries and regions and between developed and developing countries, particularly less developed countries, and that this gap is clear in the use of the Internet and the existence of connectivity[23].

In this report, the ITU also shows that, in line with the trend of individualization and personification of access and use of Internet applications, mobile communications dominate the provision of access services[24].

Being less expensive and easier to install by the use of radio frequencies, compared to the implementation of access networks by wires or cables to the user's house, wireless networks, especially mobile broadband networks, serve as the main way to have access to telecommunications networks in developing countries.

In its Global ICTs Regulatory Outlook 2017[25] (ITU, Global ICTs Regulatory Outlook 2017, 2017), ITU shows, as a trend in the telecommunications sector, that mobile communications are the

23 *International Telecommunications Union (ITU). MIS Report* – Report on the Measurement of the Information Society of the year 2017. Volume 1. (...) These divisions are evident both in the use of the Internet and in connectivity. More than half of households around the world now have access to the Internet, although the growth rate seems to have fallen below 5% per year. Households in developed countries are almost twice as likely to be online as those in developing countries and more than five times as likely as those in LDCs. There are similar differences between access rates for individual users. People in Europe are more than three times as likely to access the Internet on a regular basis as those in Africa, and are likely to benefit from faster access when doing so.

24 *International Telecommunications Union (ITU). MIS Report* – Report on the Measurement of the Information Society of the year 2017. Volume 1. (...) Mobile cellular networks are increasingly dominant and now dominate the provision of basic telecommunications services. The number of mobile cellular subscriptions worldwide now surpasses the world's population, although many people, especially in developing countries, still do not use a mobile phone. The number of fixed-line subscriptions has continued to decline, falling below 1 billion worldwide, and is particularly low in the least developed countries (LDCs).

25 *International Telecommunications Union (ITU). Global ICTs Regulatory Outlook 2017*. East *Global ICTs Regulatory Outlook 2017* It is the first in an annual series of market monitoring reports and regulatory trends in the information and communication technology (ICT) sector and its implications for the economy. Understanding current trends and challenges in ICTs markets and regulatory frameworks can help address gaps and capitalize unexplored opportunities. This report provides useful ideas and a clear and evidence-based perspective to do that. This report is also a key resource on smart, inclusive and progressive ICTs regulation. Their findings can provide a useful guide to review and update the regulatory frameworks for theICTssector as a basis for the digital economy today and for the future. The report reaches the regulatory community around the world, policy makers, the industry and the ICTs community in general.

engine for widespread Internet access.

Many elements are coming together in new and innovative ways to expand penetration: new technologies are evolving rapidly, provoking innovative business models and regulatory incentives, while consumer demand continues to exceed expectations, with the mobile sector being the engine for transforming economic sectors in general.

However, only the determination that wireless access technologies are the proposed growth of telecommunications infrastructure in developing countries does not solve the question of how to create investment conditions in these networks.

The creation of state public policies to encourage private and, where appropriate, public investment is essential if this proposal is to go beyond paper and be incorporated into each country's day-to-day life.

For developing countries, generally without a strong production chain in telecommunications infrastructure, being countries that consume equipment and, in many cases, services, confronted with a sector with a strong tendency towards concentration and monopoly, experiences show[26], after[27] years of the privatization process of the state model for the provision of telecommunications in the 1990s, that a medium-term model of the State as regulator and government formulator of public policies[28] that can be adapted economically and politically may be the way to encourage private investment in infrastructure construction.

ITU in its *Global ICTs Regulatory Outlook 2017* explains the different generations of telecommunications regulation (G1-Regulated public monopolies, G2-Open markets, liberation partial and privatization; G3-Enabling investments, innovation and access; G4-Integrated regulation, led by economic and social policy objectives; and G5-Collaborative regulation).

---

26 See references on Report MIS Report – Measurement Report of the Information Society.

27 The division between the words "State" and "Government", with the first letters in capital letters, serves to emphasize the difference between the administrative and organizational State, considered as "institutional bureaucratic structure", and political and managerial government of and in the interest of in the social organizations that work for the mechanism of democracy chosen by the majority of the population, not being the only way to build leaderships, governments and popular participation.

28 The qualifier "collaborative" is used in terms of open collaboration of all economic, political and social agents of the telecommunications /ICTs ecosystem.

Generations of telecommunications regulation

	1.Regulatory authority	2. Regulatory mandate	3. Regulatory regime	4. Competition framework
G1	Consolidated with the policy maker and / or industry	The usual	Doing what we have always done	State monopoly
G2	Separate agency	First wave of regulatory reform	Do more	Liberalization
G3	Separate, autonomous agency in decision making	Advanced liberalization of theICTssector	Doing the right things	Partial competition
G4	Separate agency with power of application	Adjacent problems become a central mandate	Doing it right	Full competition
G5	Separate agency as part of a network of associated regulators	Separate agency as part of a network of associated regulators	Do things together	Intra-modal competition

Source: *ITU Global ICTs Regulatory Outlook 2017.*

The G5 (5th generation of regulation, collaborative regulation) is the proposal of a mechanism to increase synergies between the different areas of the telecommunications sector (infrastructure and applications), creating efficiencies among the various government institutions[29], enabling a path for developing countries in the promotion of investment and the development of telecommunications networks, and, with it, the increase in access to the Internet and information.

3.4 Invisible communications: with ubiquity[30], accessibility, human training and reasonable prices

"Invisible communications" can be defined as the "mechanism" that facilitates economic and social inclusion, the driving force behind the transformation towards a more inclusive and sustainable world.

29 Ubiquity. Feminine noun. 1. Theology: divine faculty of being concomitantly present everywhere; 2. fact of being or existing concomitantly everywhere, people, things.

30 Accessibility is an essential attribute of the environment that guarantees the improvement of people's quality of life. It must be present in spaces, in the physical environment, in transport, in information and communication, including in information and communication systems and technologies, as well as in other services and facilities open to the public or for public use, both in the city as in the countryside. It is a subject that has not been widely disseminated, despite its undeniable relevance. Considering that it generates positive social results and contributes to inclusive and sustainable development, its implementation is fundamental, depending, however, on cultural and attitudinal changes. Thus, government decisions and public policies and programs are essential to promote a new way of thinking, acting, building, communicating and using public resources to guarantee the realization of rights and citizenship. See <http://www.pessoacomdeficiencia.gov.br/app/acessibilidade-0>.

As in other times where the existence of some facilitating mechanism of our life was noticed very quickly, as, for example, the existence of warming in countries with cold climate or of air conditioning or refrigerators in countries with warm climate, and that today it is considered as a normal thing and incorporated into our daily lives, sometimes not even noticed, telecommunications are being transformed into a commodity[31], with a generalized presence, acting as a basis for interaction, for economic and business development and for transformation and inclusion.

This ubiquity of telecommunications can be clearly seen in the most developed countries, where access to the most diverse forms of electronic communications is present in the daily lives of people, up to the large capacity of installed network, being based on personal interaction, but also in the realization of economic activities, such as: banking transactions, exchange and acquisition of merchandise online, commerce, commercial and industrial administration, control and monitoring, access to bases, and data analysis.

In the same way, in developing countries, this behavior is already evident, especially in large cities and concentrations of people, due, in those cases, to the greater return of private investment in the telecommunications networks that these regions make possible.

However, due to the lack of access infrastructure, it cannot be said that in all geographic regions this situation is repeated. In addition to the existence of access networks, another economic element, linked to the principle of supply and demand, is present: the price of access.

So that the fertile ground is built for the flowering of the ubiquity of telecommunications and thus allowing the appearance of the most diverse new human connections, driving the individual, spiritual and social development, it is necessary to go through the solution

31 Commodities are bulk products and raw materials, such as grains, metals, livestock, oil, cotton, coffee, sugar and cocoa, which are used to produce consumer products. The term also describes financial products, such as currencies or stocks and indexed bonds. Raw materials are bought and sold in the cash market and traded on futures exchanges in the form of futures contracts. The prices of commodities they are driven by supply and demand. When a commodity is abundant, the prices are comparatively low. When a product is scarce, the price will generally be higher. One can buy options in many futures contracts of commodities to participate in the market for less than it would cost to buy the underlying futures contracts. You can also invest through funds from commodities. See <https://financial-dictionary.thefreedictionary. com/commodity>.

of the equation "Increase access infrastructure, accessibility, human training and reasonable prices".

There has already been a bit of talk about the increase in access infrastructure, even with the indication of new regulatory formulas for developing countries to stimulate investment in the implementation of new access networks, especially with collaboration between the various economic agents and between these and the various government institutions.

With respect to human accessibility and training, these are areas where the existence of government public policies are essential for the organized and transparent management of public investments and for the planning of future actions with stability and predictability.

Special attention must be given to human training in dealing with new technologies (*digital skills*), a crucial element to allow the individual freedom and independence in the pursuit of its own and collective interests[32]. The ITU, in its Report on the Measurement of the Information Society 2017 (*MIS Report*), Volume 1, states that ICTs and other skills determine the effective use of ICTs and are fundamental to take advantage of its full potential for social and economic development. Economic growth and development will remain below potential if economies are unable to exploit new technologies and reap their benefits.

Price affordability falls into the discussion on the balance between regulation and market rules. Considering the characteristic of the infrastructure sector with tendency of concentration, aligned with the high costs of implementation of telecommunications networks, in comparison with the great dynamism of the applications sector (OTT[33]), this balance can be considered as the ideal area for the development "adjustment" by the State in the direction of a collaborative and competitive environment, being this action of

32 This is a key concept that must be studied in greater depth, as proposed in Section 5 – Conclusions and possibilities for the future.

33 OTT (Over the Top): they are the applications that turn on the infrastructures of telecommunications, in general on the Internet protocol, having different legal interpretations in each country, being in constant discussion their paper like service of telecommunications or service of added value.

the State as the natural propeller of the increase in the offer and decrease of the values collected from the users.

Equalized the above equation, a path is created for communications to be more and more present in our lives and serve, in an "invisible" way, as an omnipresent tool of transformation.

3.5 Conclusions and possibilities for the future

This study was about inclusion and social development through telecommunications / ICT, especially how communications work invisibly as a substratum to achieve those objectives.

It also involved possibilities for action by States and governments of developing countries to solve the equation for increasing infrastructure for access, accessibility, human training, and reasonable prices.

In addition, several other topics that are part of a more holistic analysis of the telecommunications sector were addressed and may be the subject of further studies in the future.

Some of these include:

- Detail of the stage in which the countries are in terms of regulations and the alternatives and paths for future development;
- Detail of options for the future relationship of the telecommunications sector and the applications sector (OTT), under the perspective of collaboration between economic agents and State institutions;
- New and innovative forms of financing, private or public, for the application of telecommunication networks for Internet access;
- Verification and investigation of best practices regarding human training in dealing with new technologies (*digital skills*), a crucial element to allow the individual freedom and independence in the pursuit of their own and collective interests;
- Determination of new areas of interest and need in human training, in the sense of social empowerment and of the individual, in face of the new possibilities offered by technological evolution;
- Regional detail, considering the particularities of each geopolitical region;

- Establishment of qualitative and quantitative investigations in the sense of validation of constructs[34] related to inclusion, personal and social development, accessibility, human capabilities, prices of services, among others;
- Specific study regarding the risks of society online, and the use of ICTs for surveillance, social control, and maximization of private interests of few dominant agents as opposed to the interest of the community.

In conclusion, the Author's wish is that these issues form the basis of a collaborative effort allows sustainable development and digital inclusion.

3.6 References

CGI. (2009). Resolución CGI.br/RES/2009/003/P. São Paulo: Comité Gestor de Internet en Brasil – CGI.br. <http://www.cgi.br/resolucoes/documento/2009/003>.

Lyon, D. (2009). Surveillance, power, and everyday life. In The Oxford Handbook of Information and Communication Technologies. Oxford University Press. <https://panoptykon.org/sites/default/files/FeedsEnclosure-oxford_handbook_3.pdf>.

Marx, G. (2015). Massachusetts. Technology and Social Control. Institute of Technology (MIT), Cambridge. <http://web.mit.edu/gtmarx/www/tech_soc_control.pdf>.

Moscovici, F. (1985). Desenvolvimento interpessoal. 3ª. ed. Rio de Janeiro: LTC.

Unión Internacional de Telecomunicaciones (UIT). (2017). Global ICT Regulatory Outlook 2017. Ginebra: Unión Internacional de Telecomunicaciones – UIT. <https://www.itu.int/pub/D-PREF-BB.REG_OUT01-2017>.

Unión Internacional de Telecomunicaciones (UIT). (2017). Informe Final Provisorio. Conferencia Mundial de Desarrollo de las Telecomunicaciones 2017 – CMDT-17, Buenos Aires, 9 al 20 de octubre de 2017. Ginebra: Unión Internacional de Telecomunicaciones – UIT. <https://www.itu.int/en/ITU-D/Conferences/WTDC/WTDC17/Pages/default.aspx>.

Unión Internacional de Telecomunicaciones (UIT). (2017). MIS Report – Informe de Medición de la Sociedad de la información del año 2017, Volumen 1. Ginebra: Unión Internacional de Telecomunicaciones – UIT. <https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017.aspx>.

34 In science, construct designates a theoretical concept that cannot be observed. Examples of constructs are personality, love, fear. Such concepts are used in the common language, but to become a scientific construct they need a clear definition and an empirical basis. See <https://pt.wikipedia.org/wiki/Construto>.

4 The Fundamental Role of the Telecommunications Infrastructure

Maryleana Mendez Jimenez

Abstract

The telecommunications infrastructure has been, is, and will be, the cornerstone on which rests the entire digital ecosystem; its goal in the 21st Century is to bring a robust, fast and secure Internet to the largest number of people, which results in the public benefit of a more connected society and the private benefit of a stronger market. The technological advance, as well as the search for the efficiency of the service provision, has generated changes in the scope, scale, ownership and amortization of this infrastructure.

In a hyperconnected world, the productive and intensive use of technology will determine the survival of business and the stability and growth of the economy as a whole. The telecommunications industry has evolved to streamline its processes and thus be able to support the strong and necessary investments in maintenance and infrastructure development, this despite being the only component of the highly regulated digital ecosystem.

Regulatory frameworks and regulators must be adapted and consolidated. In order to continue being relevant in the new economic environment, the turnaround must begin now. The role of the regulator should evolve towards a promoter of the investment necessary for the digital economy. It should also be promote healthy competition and emphasize the protection of the end users especially in terms of security and privacy.

4.1 Introduction

The fundamental objective of Telecommunications infrastructure[35] in the 21st century is to provide the service for a robust, fast and

35 Infrastructure: Underground work or structure that serves as a support base for another. Dictionary of the Royal Spanish Academy.

secure Internet at an affordable price to the greatest number of people. Depending on the service that allows to deliver to the users, infrastructure is what ultimately leads to the public benefit of a more connected society and the benefit of a market with a greater number of potential customers.

For the provision of telecommunication services, the supporting infrastructure is required[36], which includes all those passive constructive elements that allow the installation of active equipment[37], the latter being the infrastructure that enables the proper functioning of networks.

These precisions are important, since the historical evolution of both types of elements has been divergent, in the sense that the passive infrastructure has undergone few physical changes but many adjustments have evolved at the level of the business model. While the equipment has been characterized by an accelerated technological evolution, the aspects of belonging, administration and exploitation have been adjusted more slowly.

To analyze the evolution of telecommunications infrastructure over time, the following parameters will be used: scale and scope, ownership, regulation, structure of competition, amortization, and technology.

4.2 The recent past

The business model of the telecommunications infrastructure has gone hand in hand with the type of market and, therefore, the regulatory model that applies to it. At first, telecommunication networks were considered natural monopolies, it was understood at that time that it was much more efficient for a single company to be the service provider.

In the market, the retail service was limited to fixed telephony services over copper networks and dedicated links for corporate data communication. The telecommunication operators were vertically integrated, that is, they owned their own support

36 Passive infrastructure: pipelines, ducts, towers, poles, rights of way.

37 Active infrastructure: Antennas, routers, modems, replicators.

infrastructure, such as poles and pipelines, or, given their conditions of state-owned companies or private operators that operated by the State's single rating, the agreements for accessing the infrastructure of other public services.

The rights of way and installation were guaranteed and no conflict was generated with local governments or communities for their installation. It should be noted that many of these operators also had competencies for the establishment of public policies directly related to the service and the tariff setting, among others. In general, in Latin America, the scope of these networks was quite limited and very concentrated in large cities; the penetration level of voice service was only 4.5% in 1982[38]. The tariffs of the telecommunication services that allowed the amortization of the installed infrastructure were fixed, in the best of the cases, through methodologies related with cost. That is, all costs were covered, regardless of the operator's efficiency levels and a percentage of revenue was added for development as a way to fully finance the expansion projects planned for a period of time. However, because in many countries there was no independent regulator, service rates were affected by political interests and subsidies for other services[39], which ended up distorting them.

Therefore, up to that moment, vertically integrated monopoly operators were available, mostly in the hands of the State, with very low penetration and coverage networks; and mainly with a unique analogue voice service over copper pairs.

During the decade of the eighties, with the birth of mobile telephony, the monopoly vocation of telecommunications networks was being discussed.

Likewise, this is combined with serious fiscal crises that do not allow adequately financing the expansion of the infrastructure and therefore the population's demand for services is still unsatisfied.

The confluence of these technological and economic aspects, as well as the influence and momentum of intergovernmental

38 AHCIET (2008).

39 It was very common to subsidize local calls (with greater impact on public opinion) with international calls. In other words, international rates were artificially very high.

organizations[40] and international financial organizations, generated a wave of privatizations that took place in Latin America has taken place since the late eighties and during the nineties[41], opening the door to private capital of investment in telecommunications network infrastructure.

At this point, it is necessary to bear in mind that the emergence of mobile telephony was a technological advance that implied a substantial change in the telecommunications market and in the type of infrastructure required for the provision of the service. Due to its technical characteristics, mobile telephony requires the installation of antennas that allow receiving and transmitting the waves of the radio electric spectrum, a finite natural resource, which is assigned by the State. These antennas must be located in predetermined places by the network technical design, so that the objective of having the greatest possible coverage is achieved. At the same time, they need to be supported by structural elements in the form of towers or similar that have the necessary height to achieve a better use from the point of view of site connectivity.

The spaces where the towers are located must comply with the existing legal regulations in the different territories, namely: network planning, safety, sanitation, and urban planning. This shows the important role that local governments have had and still have in the development and expansion of telecommunications infrastructure.

It is important to mention that civil society in Latin America, due to unfounded concerns related with health and urban planning, has staged protests against the installation of passive telecommunications infrastructure, which has caused local governments establish restrictive measures for the installation of this infrastructure. This has led to the paradox that as more connectivity and better quality of service is required, it becomes very complicated and in some cases impossible; and, of course, it makes its deployment more expensive and therefore the service itself.

---

40 The WTO and the ITU played a fundamental role in the privatization processes seeking the standardization of processes as diverse as the institutional design of the public entities of the Telecommunications Sector, roles and responsibilities, numbering plans, interconnection, universal service among others. See <https://www.wto.org/english/tratop_e/serv_e/telecom_e/ tel23_e.html>.

41 The first countries Chile 1989, Argentina 1990 and Venezuela 1992

> *"This necessary investment, however, has been slowed in some cases at the local level since in the Latin American context there are many legal and regulatory restrictions or regulatory gaps to install infrastructure, mainly basic antennas and equipment required by the network a situation that unfortunately affects the increased coverage and capacity required for the deployment of mobile telecommunications services*[42]*."*

Up to this point, the ownership of the infrastructure was decisive in order to achieve positions within the markets, and therefore the measures to promote competition necessarily circulated through the sharing of this infrastructure, which generated conflict with established operators[43] in the market for the recognition of the investments made.

The passive infrastructure receives the treatment in the regulatory norm of scarce resource, that is to say that they are resources that are limited by their physical or urbanistic capacities; it is possible to mention that they receive this same treatment, the radio electric spectrum and the numbering. Given the essential function of these resources within the provision of telecommunications service, Its efficient use must be guaranteed and it is assumed that the regulatory obligations that could be imposed should be limited to what is strictly necessary for the proper operation of the service and avoid monopolistic practices; however, the intervention of the regulator for access and sharing, both in poles as in ducts and towers, at a regulated wholesale price was imposed.

Ideally, in modern regulation the regulator's action in terms of access to passive infrastructure should be subsidiary, that is, on the one hand, negotiation between parties is privileged and, in addition, there is intervention by the regulator only when there is an unjustified refusal to negotiate or access by the operator that owns the infrastructure. The regulator goes rather to resolve conflicts, instead of imposing ex-ante measures that tend to be very burdensome and negative for the development of the sector.

42 cet.la (2015).

43 See examples in Agüero (2013) and Prensario Internacional (2016).

4.3 Ephemeral Present

In the new millennium, technological evolution causes a market shift. First, the paradigm is broken in a definitive way that the network could not be replicated, since the market already has alternative networks developed by cable operators and mobile operators. Convergence, that is, the possibility of providing various services through the same network, is a reality and also opens a new competitive edge, since it enables the possibility of accessing the Internet from mobile devices.

4.3.1 A predominantly mobile access

Access to broadband in Latin America is mainly mobile. The technological evolution towards new generation of active infrastructure elements that enable access to the mobile Internet and the democratization of this access thanks to the pre-paid models have made it possible to considerably expand the penetration of this service. According to ITU[44]. In 2016, 51.3% of the average Latin American population has access to mobile internet, on the other hand, only 8.94% on average have a fixed Internet access connection. Likewise, of these accesses, around 80% are prepaid connections against 20% postpaid. Despite these advances, 48.7% of Latin Americans still do not access the internet.

As the penetration of the service has increased, the ARPU has also decreased[45] from Latin America, standing at 9.6 dollars per user per month in 2015, which is below other regions such as North America with an ARPU of $ 49.1 per user per month and $ 31.8 per user per month in Western Europe. In this sense, the combination of slower economic growth, greater pressures in terms of competition and increasing regulatory obligations focused mainly on traditional actors, has generated pressure on the ARPU levels. Throughout the region, ARPU registered, on average, a fall of 2.6% per year, in dollars, between 2010 and 2015, and it is projected that another 2.8% per year will fall through 2020[46].

44 ITU (2017).

45 ARPU – From English Average Revenue per User – Average income per user. The ARPU is the average or average revenue per user that obtains, in a period, a service company with a broad user base. It is calculated by dividing the total income obtained in the period, among the total active users of the company. See <https://es.wikipedia.org/wiki/ARPU>.

46 GSMA (2016).

4.3.2 The emergence of Digital Services over the Internet

Technological innovation generates a competitive element that, in a disruptive way, has a direct impact on the business model of telecommunications operators and, therefore, on the amortization of infrastructure. This is the emergence of digital services on the Internet called "*Over the TOP*"(OTTs). These applications revolutionized the way we consume services. If we circumscribe it only to telecommunications services, the applications have made very profitable traditional services such as international calls and text messages, notably decrease by users in a very short period, since some of these services work in practice as substitute services. To mention an example, in Costa Rica between 2004 and 2015 international calls went from 160 minutes per user per year to less than 40 minutes per user per year; consistently the SMS went from 8,000 million SMS per year in 2009 to less than 1,000 million in 2015, this entails moving from 382 SMS per user per year to 19 SMS per user per year[47].

It is also notable how revenues from both fixed and mobile voice services have been decreasing, while data consumption continues to increase in a curve that has an exponential trend. In this sense, it can be highlighted that the data traffic per user per month will increase from just over 0.5 GB per month in 2015 to almost 4 GB in 2020[48].

We must pay attention to the fact that digital services, in the analysis of telecommunications markets, have not been considered as substitutes for telecommunications services because "... *It is considered that OTT applications are not yet constituted as substitutes for traditional services since* ***they do not provide a means of access*** *service*[49]*".* However, the impact on the use of traditional services begins to show up in the statistical information.

However, many hypotheses can be raised about whether it was the strong penetration of telecommunications networks that allowed digital services to emerge and spread, or whether digital services promoted the adoption of Internet services. The truth of the matter

47 Superintendence of Telecommunications (2016).

48 GSMA (2016).

49 Superintendent of Teleommunications.

is that we are in the presence of a typical case of interdependence: "The reason for change in the value chain is due to the technical progress that has given rise to a totally different sector, the digital ecosystem, in which telecommunications represent only a part of the chain, and not the most important economically, although it is the only one that is regulated"[50].

4.3.3 New business models

Digital services have not been considered telecommunication services as they are not yet studied as substitutes for them. Therefore, they have not been subject to sectoral regulation, but they directly impact the demand for services and the income of operators, which are subject to a regulatory framework that has not evolved with the same speed as technology.

What is clear is that not all direct services delivered to end users through the installed infrastructure contribute to their amortization, as it was the business model that originated the regulation that still applies.

To measure the investment, which means the maintenance of the existing infrastructure and the development of new networks, in Latin America in 2014 the gross production of the telecommunications industry was 147.8 billion dollars and generated an added value of 68,468 million dollars, of which 43% went to these items, that is, 29.441 million dollars[51].

Under these market circumstances, with competitive pricing, well-consolidated digital services, growing penetration, falling ARPU, very high bureaucratic complexity for the use and development of passive infrastructure, and regulatory pressure, operators are faced with the need to continue investing in their networks and also reduce their operatives costs to stay competitive. This has generated a new business model, where companies that convert the administration and construction of infrastructure into their core business enter the ecosystem.

50 Crisanto (2015).

51 Katz (2017).

With a real estate model, companies like Tower One[52], Telesites[53] and SBA Communications[54], acquire the infrastructure sites already developed by telecommunications companies and develop their own sites for rent. This business in a natural way makes available the infrastructure for as many operators as technically allows the physical structure and facilitates that the telecommunications companies concentrate on their main business.

From the regulatory point of view, this is a kind of "voluntary structural adjustment". It can be said that a lot of the passive infrastructure, in Latin America, 49%[55] out of a total of 167,371 towers, telecommunications poles and rooftops, is in the hands of companies not subject to sectoral regulation, to which obligations cannot be imposed. However, the telecommunication services continue to be highly regulated.

In parallel, some countries try to improve their response capacity through laws and regulations building networks to meet the needs of the population in terms of connectivity, such as Peru with the Law of Strengthening for the expansion of the telecommunications infrastructure[56,57]. These regulations establish that the public interest of telecommunications services must prevail throughout the territory. However, the problems to obtain construction permits persist and in many countries the local government politization of the decisions continues to prevent the adoption of better practices for the development of infrastructure.

What is clear, as already mentioned, is that in order to share infrastructure whether outsourced or propietary, there should be a privileged negotiation between parties before a regulatory intervention that can lead to a slowdown in investment[58].

It should be noted that telecommunication operators are only in the wholesale segment who install neutral fiber networks that are offered

52 See <http://www.toweronewireless.com/>.

53 See <https://www.telesites.com.mx/>.

54 See <http://es.sbasite.com/>.

55 TowerXchange (2017).

56 Peru (2015).

57 Ibid.

58 Jung (2017).

to operators at market prices, allowing a better use of infrastructure resources, and they have extended these outsourcing models, such as passive infrastructure, to the installation of new generation networks.

4.4 Conclusions: Near future

The current industry conditions and the constant technological innovations mean that speaking only about telecommunications is focusing in one of the components of a much more complex ecosystem, which is the basis for the digital economy. This ecosystem is now made up of companies of different technological nature. It is an interdependent community with a complex dynamic, where the interventionist rules from the states are obsolete, not only because the business development environment is much broader, but also because the survival of its members who are in charge of the infrastructure depends on there being no barriers to compete and that public policies, far from limiting, would encourage investment and the protection of the rights of end users.

It is foreseen that with the mobile fifth generation (5G), technology that is still in the process of standardization, the amount of connected devices will increase considerably, it is estimated that there will be 3.3 billion connections of Internet of Things (IoT) in 2021[59]. Consequently, there will be a need to increase the amount of infrastructure necessary to support these levels of connectivity. In addition, the radio bands of spectrum already identified for the new technology are high frequency bands, which will also influence the density of the infrastructure. In this context "... to reach the 20 Gbps or more planned for 5G, we will require carriers of 200MHz or 400 MHz of bandwidth, which are only available in frequencies above 5 GHz"[60]. If there was already a challenge to develop and maintain the infrastructure, this is broadened by a matter of scope and density of the networks that will support this technological advance.

Also, telecommunication operators, in an effort to continue the process of adapting their business to the new features of the environment, are betting on making their networks more efficient, considering a key element the virtualization of the "core" of these networks and

59 Cisco (2017).

60 Rysavy Research (2017).

even of some elements of the access network. Virtualization refers to implementing the functions of the infrastructure nodes with software on commercial computer equipment.

This model promises lower capital costs, lower operating costs, faster implementation of new services, energy savings, and an improvement in network efficiency"[61].

With this virtualization, the active elements in the cloud will be able to distribute their processing capacity in the most appropriate way: according to the demand of their users. For the first time it will be seen how the cloud will be defining itself, with the aim of procuring response times close to zero in order to support the critical devices that will be connected. This is another step in the process of "lightening" the business model of telecommunications network operators, which is essential to be able to compete.

We will live in a hyperconnected world, with self-adjusting networks, where the competition will be directly related to the value that is delivered to the client and the adjustment of the solution to their needs. The productive and intensive use of technology will determine the survival of business and the stability and growth of the economy as a whole.

Regulatory frameworks and regulators in turn must adapt and consolidate. To continue being relevant in the new economic environment, the turnaround must begin now. Latin America should make a productive use of new digital technologies and focus on the installation of infrastructure to make this viable. The role of regulator should evolve towards a promoter of the necessary investment for the digital economy; it should also be vigilant that there is healthy competition and should emphasize the protection of the end user especially in terms of privacy and security. Special emphasis should be given to investment in rural areas, where an appropriate public-private effort will be necessary to achieve the universalization of the service to make the benefits of the new economy reach all the inhabitants.

A change of this magnitude requires the contribution of all.

61 Ibidem.

4.5 References

AHCIET (2008). ¨Telecomunicaciones en Iberoamérica.¨ Montevideo, Uruguay.

Agüero, M. (2013, 9 maio). Arriendo de postes enfrenta a firmas de telecomunicaciones. La Nación. <https://www.nacion.com/el-pais/servicios/arriendo-de-postes-enfrenta-a-firmas-de-telecomunicaciones/ZEBAPFUTGRAA5FFXWYRG7UGDFY/story/>.

cet.la – Universidad Externado de Colombia (2015). Guía de Servicios móviles de Telecomunicaciones.

Cisco (2017). Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016-2021.

Costa Rica (2009). Ley General de Telecomunicaciones. Ley No. 8642.

GSMA (2016). "La Economía móvil en América Latina". <https://www.gsma.com/latinamerica/wp-content/uploads/2016/09/ME_LATAM_2016-Spanish-Report-FINAL-Web-Singles-1.pdf>.

Jung, J. (2017). Los riesgos de mandatar la compartición de infraestructura. Mediatelecom.

Katz, R. (2017). Retornos y Beneficios del Sector Telecomunicaciones. cet.la. Montevideo, Uruguay.

Perú (2015). Ley de Fortalecimiento para la expansión de la infraestructura de telecomunicaciones y sus modificaciones. Ley No 29022.

Plaza, C. (2015). Ensayo sobre la Regulación Tecnológica, La era digital en Europa. Barcelona, España.

Prensario Internacional (2016, 5 agosto). Costa Rica: Preocupa a operadores la falta de acuerdo con dueños de infraestructura. <http://www.prensario.net/17057-Costa-Rica-Preocupa-a-operadores-la-falta-de-acuerdo-con-duenos-de-infraestructura.note.aspx>.

Rysavy Research (2017). LTE to 5G Cellular and broadband innovation. 5G Americas. <http://www.5gamericas.org/files/6415/0282/1551/2017_5G_Americas_Rysavy_LTE_5G_Innovation__Final_for_Upload.pdf>.

SUTEL Superintendencia de Telecomunicaciones (2016). Estadísticas de Mercado. Presentación para el Foro Regional de Competencia OCDE. San José, Costa Rica.

SUTEL Superintendencia de Telecomunicaciones (2017). RCS-248-2017 Revisión del mercado del servicio minorista de telecomunicaciones móviles, análisis del grado de competencia en dicho mercado, declaratoria del operador y/o operadores importantes e imposición de obligaciones. San José, Costa Rica.

TowerXchange (2017). CALA Towers Spotlights on the CALA tower industry. American Dossier. <https://www.towerxchange.com/wp-content/uploads/2017/05/TX_CALADossier_2017-1.pdf>.

União Internacional das Telecomunicações (UIT) (2017). Estadísticas 2016. Ginebra, Suiza.

5 The Challenges of Internet Access

Oscar Robles Garay

Abstract

The unconnected represent 50% of the planet's, including the most vulnerable and geographically isolated groups, which implies a greater challenge than what meant connecting the first half of the population during the last 30 years However, this could not be an excuse to ignore the challenges that also exist with those already connected, challenges that also establish moving and growing targets in the coming years, which require a suitable Internet for the tasks we face today and an open Internet as the open Internet has been the one that has stimulated this global dynamism that we enjoy today. This article explores the challenges that are present in any country, not only for the less developed ones, hence the importance of keeping them in our discussions with the aim of establishing sustainable solutions.

5.1 Introduction

When we talk about the challenges of Internet access we have to focus on connecting the non-connected. They not only represent 50% of the population of the planet[62], but also in that percentage are located the most vulnerable groups and in geographically isolated areas, which implies a challenge superior to what has been connecting the first half of the population during the last 30 years.

However, the above could not be an excuse to ignore the challenges that exist with those already connected – challenges that also set moving and growing targets in the coming years, which require an Internet suitable for the tasks we face, and an open Internet proven responsible for the global dynamism of today. These challenges are present in any country, not only for the least developed ones, hence the importance of maintaining them in our discussions with the objective of establishing sustainable solutions.

62 See IWS (2017).

5.2 Quality access for those already connected

Those already connected require quality access. This has two fundamental aspects: on the one hand, we have to talk about Internet connectivity, and on the other hand a more complex concept, but no less important, which is a quality Internet access.

Internet connectivity is not just being connected certain hours per day, it refers to a certain bandwidth that allows to have most of the online resources at a reasonable time and cost, not only for entertainment and information purposes, but as an enabling tool for human rights; such as the possibility of having access to quality education content that complements the local education offer and in some cases as the only way of training in technology. A bandwidth should not only allow access information in social networks but should also allow innovative and creative ideas of services and solutions to society's needs.

We are referring to broadband, a term that is dynamic, but even the International Telecommunications Union in its most recent Information Society Report[63] define it as 256 Kb/s:

> *The second long-term trend is the growth in broadband – defined in this report as services with speeds of 256 kbit/s and above*

And it has failed to update it since it has been used at least since 2003[64].

> *Recommendation I.113 of the ITU Standardization Sector defines broadband as a transmission capacity that is faster than primary rate ISDN, at 1.5 or 2.0 Mbit/s. Elsewhere, broadband is considered to correspond to transmission speeds equal to or greater than 256 kbit/s, and some operators even label basic rate ISDN (at 144 kbit/s) as a "type of broadband". In this report, 256 kbit/s is generally taken as the minimum speed.*

And even when someone can argue this bandwidth as adequate, it is clearly arguable why it has remained the same for 14 years. What today is considered as broadband, within a couple of years

63 See ITU (2017).

64 See ITU (2003).

may be insufficient for the purposes mentioned above. This applies to the mountains in Haiti or to a prominent neighborhood in Norway. It is undeniable that the risk of obsolescence is greater in less developed economies, but the truth is that all the current indicators that measure Internet access in different countries are binary[65], indicating how many are connected or not, and how many of those connected have broadband. Those who publish these indicators assume that this percentage of broadband connected will only increase in the coming months, and this may not the case.

The indicators should seriously consider the speed of the access each community receives in relation to an acceptable minimum for the proper use of the Internet, how many below that acceptable minimum, how many just above, and how many with sufficient bandwidth, and make sure to update the indicators consistent with the acceptable minimum. This would allow us to know the evolution or degradation of access over time for a specific community and not, what usually happens, that only happy inferences are made of how many more were connected, which generates a false sense of technological development.

We could try to establish an even stricter criterion for establishing an Internet bandwidth in which a minimum "upload" speed is defined, fundamental for technology business entrepreneurs and even for multiparty video calls that could benefit teleworking or self-employment in our countries, but none of this is possible because we do not measure it and we do not know the status of these indicators. What we lose are not only interesting details for those fascinated by technology, but the chance to promote these work and professional activities, or to generate national strategies that stimulate them.

---

65 The Index of development of Information and Communication Technologies published by the International Telecommunication Union since 2009 (Global ICTs Development Index) considers the following indicators to measure "Preparation for ICTs" (ITC Readiness) and "Intensity of ICTs" (ITC Intensity):
a) fixed-telephone subscriptions / 100 inhabitants
b) mobile-cellular telephone subscriptions / 100 inhabitants
c) international Internet bandwidth (bits/s) per user
d) percentage of households with a computer
e) percentage of households with Internet access
f) percentage of individuals using the Internet
g) fixed (wired) -broadband subscriptions per 100 inhabitants
h) Wireless broadband subscriptions per 100 inhabitants (includes satellite, terrestrial fixed, and active mobile with a minimum download of 256 kbit/s)

When we talk about a quality Internet, in addition to broadband or access speed, we have to talk about the quality of the Internet itself. Note that the Internet represents the ability of a device to use[66], 536 different possibilities for "going out" to the Internet, options that are technically known as "ports". Each time we use an application on the Internet, it is configured to use some of those ports to get the content. However, many current services significantly restrict these possibilities. Services such as Zero Rating, which constraints access to a few pages on the Internet[67], Technologies such as Network Address Translation (NAT) or Carrier Grade NAT (CGN), or content and application restriction policies by operators or central authorities that restrict entire pages or the number of ports that applications can use, all silently affecting the quality of the Internet that a user receives. Silent, because the average user is not aware of this limitation, and at some point could even get used to it[68], because no one in which they account for Millions of Facebook users who have no idea of using the Internet. misses what they have not known, and could live with this limited set of options (of pages or ports) without taking advantage of an important fraction of the Internet, fundamental for the full exercise of rights such as the right to quality information, or even to favor technological innovation by creating applications that require and exploit a significant amount of possibilities on the Internet.

And in general, in order to achieve a quality Internet, we must maintain an Internet that largely addresses the fundamental principles that have made it successful and that have helped billions of people today to enjoy their right to information, to education, to freely share the fruits of their innovation and creativity, and to have access to job offers outside their place of residence. That Internet has been mutating and some fears caused by security threats have been pruning it. As a result, we have been seeing more limited access to the Internet. Thus, states will have to be very aware that the restrictions they impose on an open Internet can affect

66 For an analysis of zero rating practices, see ISOC (2016).

67 For an analysis of zero rating practices, see ISOC (2016).

68 For an analysis of zero rating practices, see ISOC (2016).

the Internet more than they can imagine and thus the economy generated by this medium. It is not a minor issue for the states if we consider the contribution that the digital economy represents in the gross national product.

All these challenges, an adequate amount of bandwidth and an Internet of quality, represent an additional complexity for two reasons: first because they are moving targets, what today may seem to be solved, tomorrow may not be totally or partially solved, and secondly because we do not have them "in sight", unlike the most well-known challenges such as bringing access to the disconnected who are very present. Therefore, its relevance, to the extent that we are aware of these challenges, more possibilities we will have to address them in an appropriate manner.

5.3 Keep connected to the connected

It is common to find in some countries unsustainable Internet access projects, which exist only "to show off" very expensive projects in their operation, which seems to be irrelevant upon evaluation and only considers the communicational impact at the moment of its release.

The problem is that there are communities that rely on these projects to gain access, and once the opening lights of the project are gone, these communities will have major problems to keep that Internet access project running.

During one of the recent Internet Governance Forums (IGF) I had the opportunity to note this situation. I was in a public square where they were announcing a national free connectivity project, when I tried to connect to this network. The Service Set IDentifier or SSID was not even being announced; probably the access equipment was not even connected anymore. This was only 18 months after the project was inaugurated, a few steps from the financial district of one of the most important cities in the country we visited. What could we expect to happen in the marginal areas of that city? What could we expect to happen in the marginalized geographical areas of that country? What could we expect to happen in a country with less possibilities of development?

As it is usually said, "It is not possible to improve what cannot be measured". In this case, we are interested in at least ensuring that certain levels of Internet quality are maintained for those already connected, but we won't be able to ensure it as long as we do not adequately measure these indicators.

5.4 Those others not connected

The debate of connecting the unconnected is dominated by the challenge of those geographically distant from urban centers, but the isolation is not only geographical. In order to have the complete representation of the problem we must also take into account the age isolation, the isolation due to physical or cognitive disabilities, the marginalization by socioeconomic level, and the barriers by gender, among others.

Even when there are sustainable access solutions for geographically dispersed or complicated areas, these will not connect most of these groups, who share with each other the bad fortune of not being a business case for anyone. Therefore, the solution to many of the previous challenges will not be isolated commercial ideas to serve a niche, but solutions with the participation of various types of actors with different levels of involvement.

That is, connecting to the visually impaired will be ineffective if there are no holistic solutions to their incorporation into educational possibilities or a labor market that allows them to be self-sustaining.

The previous statement does not prevent the emergence of commercial solutions that attend the needs of these vulnerable or isolated groups. It is perfectly valid that commercial organizations have among their services one that can meet those needs. While we cannot expect that to be the only solution, it is highly likely that solutions will never come by this route. Nor can we expect the welfare state to satisfy all these needs because it does not have the creative capacity, the efficiency, the multiplicity of ideas and the collaboration between diverse entities that are often required to address these challenges.

Some examples of creative solutions to these needs are found in Argentina, with the Free Router project of AlterMundi[69] that has achieved to connect geographically dispersed rural areas; or community networks in southern Mexico, in Oaxaca[70] In both cases and without government intervention they managed to establish a network operated by their own means and in a sustainable manner.

In that same sense, the United Nations Declaration on the Rights of Indigenous Peoples[71] states in article 16:

> *Indigenous peoples have the right to establish their own media in their own languages and to have access to all forms of non-indigenous media without discrimination.*

Which, at the same time, establishes an obligation to the State to provide the necessary facilities for these communities to attend that right. It is therefore essential that each sector of society assume a part of the responsibility and together seek sustainable solutions for these groups.

5.5 The unknown of the already known challenges

Finally, it is important to identify the unknown aspects of the known challenges. We are talking about IPv6, an essential technological resource when we talk about the challenge of connecting the non-connected.

Currently, we have the challenge of connecting nearly 250 million people to the Internet in the Latin American and Caribbean region, however we only have a little more than 3 million IPv4 addresses71 (Internet Protocol version 4) available, making it impossible to connect those 250 million people, unless the operators use the new definition of Internet Protocol known as IPv6[72] (Internet Protocol version 6). Some operators in the region have had the

69 See Redesac (2018).

70 See Redesac (2018).

71 See the English version in UN (2008), since the Spanish version reduces the "media" concept to "information media" only; when most dictionaries in English consider this term broader: "The main means of mass communication (broadcasting, publishing, and the Internet) considered collectively".

72 See Postel (1981).

need to use technologies to take advantage of their old addresses (NATs, CGNs, etc.) to connect their new customers. Today, there are technological mechanisms that use IPv6 (one is 464xlat[73]) that allow these operators to put aside their old addresses (and with it the NATs and CGNs) for certain types of clients, with which they can even be assured of an Internet of quality like the one we talked about in previous paragraphs.

Governments (the state) play a fundamental role in promoting IPv6 in their respective regions by being a major buyer of technology. With the mere fact of requiring IPv6 compatibility in the technological solutions they acquire, they are able to stimulate the supply of diverse services compatible with IPv6. Once Governments understand that role, it will be possible that telecommunication operators may have among their services, Corporate DSL (Digital Subscriber Line) or Fiber, any of them with native IPv6, that network equipment vendors consider relevant and commercially viable to include in the firmware of routers, switches and CPEs (Customer Premises Equipment such as modems, cable modems, radios) compatibility for IPv6 and finally for the various network solution providers it will be attractive to offer network design and configuration solutions compatible with IPv6. And also very important, the industry together with the academia should start developing the necessary talent to maintain all these services.

Therefore, and given its technological complexity, it is important for governments to be aware of these challenges that for some are still unknown. In recent years it has ceased to be a purely technological one and today is not even a purely commercial issue. Today it is a strategic challenge for the development of the countries, because as we mentioned before, it is fundamental to connect the disconnected.

5.6 Conclusions

Connecting the other half of the world is a huge challenge that can only be addressed with the involvement of multiple actors in

73 See Deering and Hinden (2017).

each region. The state cannot be solely responsible for meeting this challenge, nor does it seem feasible to think that traditional Internet access providers modify their nature and begin to expand infrastructure in areas where there is no return on investment and overnight, pay attention to areas or communities that have not been served for decades.

However, it is essential to bear in mind that this challenge implies additional considerations, since it is not "any Internet" that will resolve the digital divide, just as it has not been "any Internet" that has caused the global dynamism that we enjoy today. It is an Internet of quality and in enough quantity which will make most of the resources be ubiquitous for any user and only then, with an Internet of sufficient quality and quantity, it will be useful for the development of societies.

5.7 References

AlterMundi (2017). Proyecto Libre Router. <http://programafrida.net/archivos/project/router-libre y <http://docs.altermundi.net/>.

Deering S. y Hinden R. (2017). Internet Protocol, Version 6 (IPv6) Specification. Internet Engineering Task Force. Request for Comments: 8200. <https://tools.ietf.org/html/rfc8200>.

Internet Society (ISOC) (2016). Policy Brief: Zero-Rating. <https://www.internetsociety.org/policybriefs/zerorating/>.

Internet World Stats (IWS) (2017). Internet World Penetration Rates by Geographic Region. <https://www.internetworldstats.com/stats.htm

Mawatari, M.; Kawashima, M.; Byrne C. (2013). 464XLAT: Combination of Stateful and Stateless Translation. Internet Engineering Task Force. Request for Comments: 6877. <https://tools.ietf.org/html/rfc6877>.

Organización de las Naciones Unidas (2008). United Nations Declaration on the Rights of Indigenous Peoples (versión en inglés). <http://www.un.org/ esa/socdev/unpfii/documents/DRIPS_en.pdf>.

Postel, J. (1981) Internet Protocol. Internet Engineering Task Force. Request for Comments: 791. <https://tools.ietf.org/html/rfc791>.

Redesac (2018). Redes Por la Diversidad, Equidad y Sustentabilidad A.C. <https://www.redesac.org.mx/single-post/2018/02/02/La-instalaci%C3%B3n-del-s%C3%A9ptimo-nodo>.

Mirani, L. (2015). Millions of Facebook users have no idea they're using the internet. Quartz. <https://qz.com/333313/milliions-of-facebook-users-have-no-idea-theyre-using-the-internet/>.

Unión Internacional de Telecomunicaciones (UIT) (2017). Measuring the Information Society Report 2017 (Pag. 4). <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf>.

Unión Internacional de Telecomunicaciones (UIT) (2017b). Global ICT Development Index. <http://www.itu.int/net4/ITU-D/idi/2017/>.

Unión Internacional de Telecomunicaciones (UIT) (2003). ITU Birth of Broadband 2003. <https://www.itu.int/osg/spu/publications/sales/birthofbroadband/exec_summary.html>.

6 The Evolution of Telecommunications: Technology, Public Policies and Regulation in Argentina

Agustín Garzón

Abstract

The evolution of telecommunications has generated a dynamic development of ICT Services and applications, which include traditional telephony and broadcasting services as well as new digital services, based on the Internet, that lead to the analysis of current issues such as Regional Digital Market, Artificial Intelligence, Industry 4.0, Cybersecurity and 5G, among others.

Likewise, the development of telecommunications has tended towards technological convergence, allowing the provision of different services through the same telecommunications infrastructure, which requires a regulatory framework that favors and encourages the development of the sector, and allowing users to access a greater offer of services, in an affordable way and in equitable social and geographical conditions. In order to achieve the aforementioned objectives and generate a suitable environment for the implementation of telecommunications / ICTs services, an adequate telecommunications infrastructure is needed and that is why public policies are focused on the deployment of infrastructure.

In the present article the main technological trends are detailed, as well as the regulatory tools that favor their implementation. Also, the main difficulties faced by the sector and the regulatory measures and public policies developed with the aim of resolving them are described.

6.1 Introduction

In recent years, the evolution of telecommunications and Information and Communication Technologies (ICT) have allowed the development of innovative services and applications.

Recognizing that the aforementioned development has tended towards a technological convergence, also generating a convergence of services, which allows the packaged marketing of services under

the figure of N-Play, the National Communications Agency (ENACOM) was created in Argentina through the Decree 267/2015.

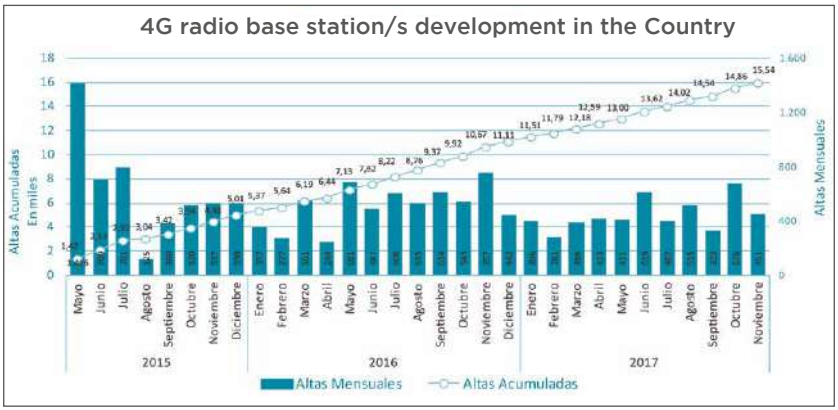
The ENACOM is then empowered to establish a regulatory framework that allows adequate conditions of development of the industry corresponding to the telecommunications /ICTs and broadcasting sectors, which were previously regulated by different bodies. This results in a favorable environment for the convergence of services, for the benefit of the users, with the objective that they can access a greater diversity of services at lower prices as a result of the increase in competition.

On the other hand, Argentina is involved in the development of public policies in telecommunications, participating in the main Forums and International Organizations, such as the International Telecommunications Union (ITU), the Inter-American Telecommunications Commission (CITEL), the G20 (industrialized and emerging countries), the Organization for Economic Cooperation and Development (OECD), the Latin American Forum of Telecommunications Regulatory Entities (REGULATEL), the Internet Governance Forum (IGF), among others.

In the case of the G20, Argentina held the presidency of said Forum in 2018 promoting digital inclusion, while in relation to the OECD, Argentina works energetically to complete the admission process as a member of that organization. In the case of CITEL, Argentina will organize the next Assembly in Buenos Aires and will assume the presidency of the Permanent Executive Committee of CITEL (COM / CITEL). The Assembly establishes the policies for the fulfillment of the objectives and functions established in the Statute, such as acting as a Senior Adviser Body to the OAS in the field of telecommunications and to undertake studies and programs to promote the development of telecommunications / ICT, among others.

Likewise, the current digital agenda includes diverse topics such as the Regional Digital Market, the Global Digital Economy, Artificial Intelligence, Industry 4.0, Internet Governance, Cybersecurity and 5G, among others, which are in full debate and development. In this sense, in order for all this to be possible, an indispensable requirement is needed: to support these developments on the basis of an adequate telecommunications infrastructure. That is why public policies in telecommunications are centered on the deployment of said infrastructure.

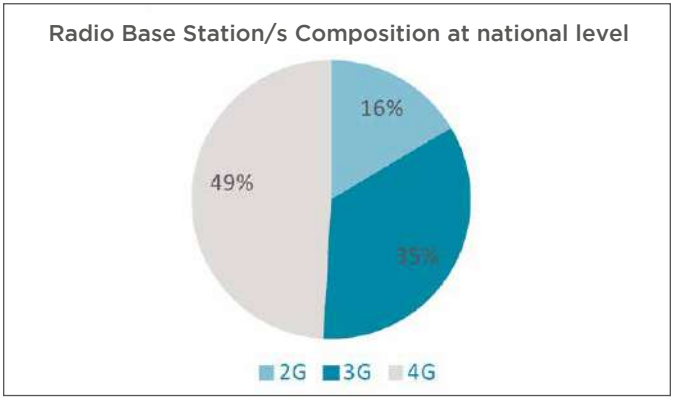
In order to be able to make an approximation of the evolution of infrastructure deployment since 2015, the following graph shows the record of 4G base stations in Argentina:



Source: ENACOM

It can be seen that from the beginning of 2015 to the present, approximately 16,000 radio bases with LTE technology were deployed nationwide.

In relation to the total number of base stations, those that operate with 4G technology have been deployed since 2015, currently making up 49% of the total, so it can be seen that from 2015 to 2017 the number of base stations has doubled those of the mobile service, without considering the new radio base installations with 2G and 3G technologies.



Source: ENACOM

In the regional context, the number of broadband mobile subscriptions disaggregated by 3G and 4G technologies, according to what was released by OVUM, has evolved between 2015 and 2016 in some countries of the region as shown in the following table:

Argentina

Generación	1Q15	2Q15	3Q15	4Q15	1Q16	2Q16	3Q16	4Q16	Evolución 2015-2016 (%)
3G	23.106.089	23.953.008	24.504.515	28.402.707	28.691.715	28.972.960	29.138.010	28.887.527	25
4G	788.430	1.117.362	2.030.465	4.290.301	6.536.511	7.291.807	9.648.683	11.913.206	1411
Total	**23.894.519**	**25.070.370**	**26.534.980**	**32.693.008**	**35.228.226**	**36.264.767**	**38.786.693**	**40.800.734**	71

Brasil

Generación	1Q15	2Q15	3Q15	4Q15	1Q16	2Q16	3Q16	4Q16	Evolución 2015-2016 (%)
3G	164.205.800	169.524.430	166.298.883	155.026.605	151.072.504	143.836.540	136.279.350	123.595.423	-25
4G	9.240.617	13.379.788	18.520.081	25.716.918	32.816.256	40.005.977	49.692.823	60.448.215	554
Total	**173.446.417**	**182.904.218**	**184.818.964**	**180.743.523**	**183.888.760**	**183.842.517**	**185.972.173**	**184.043.638**	6

Chile

Generación	1Q15	2Q15	3Q15	4Q15	1Q16	2Q16	3Q16	4Q16	Evolución 2015-2016 (%)
3G	9.573.117	11.730.532	13.404.018	14.008.208	15.105.296	14.929.187	15.712.246	16.281.019	70
4G	1.173.765	1.482.737	1.921.156	3.092.022	3.768.234	4.263.235	4.760.020	5.429.572	363
Total	**10.746.882**	**13.213.269**	**15.325.174**	**17.100.230**	**18.873.531**	**19.192.423**	**20.472.266**	**21.710.591**	102

Colombia

Generación	1Q15	2Q15	3Q15	4Q15	1Q16	2Q16	3Q16	4Q16	Evolución 2015-2016 (%)
3G	12.565.826	13.441.131	15.935.792	22.443.827	22.692.209	23.773.779	25.852.388	28.010.068	123
4G	2.016.465	2.572.419	3.273.717	4.416.532	4.987.691	5.993.311	6.826.626	7.662.577	280
Total	**14.582.291**	**16.013.550**	**19.209.509**	**26.860.359**	**27.679.900**	**29.767.090**	**32.679.014**	**35.672.645**	145

México

Generación	1Q15	2Q15	3Q15	4Q15	1Q16	2Q16	3Q16	4Q16	Evolución 2015-2016 (%)
3G	33.361.303	34.286.048	39.104.936	44.725.177	46.908.612	46.900.731	48.014.041	50.121.843	50
4G	2.275.498	3.792.051	5.085.859	7.050.205	8.898.089	11.048.257	12.279.410	15.660.583	588
Total	**35.636.801**	**38.078.099**	**44.190.795**	**51.775.382**	**55.806.702**	**57.948.989**	**60.293.452**	**65.782.426**	85

Source: ENACOM

It can be observed that user´s penetration of mobile services with 4G technology has grown strongly in the region during 2015-2016, Argentina being one of the countries with the faster adoption, going from approximately 800,000 subscriptions to almost 12,000,000 in two years.

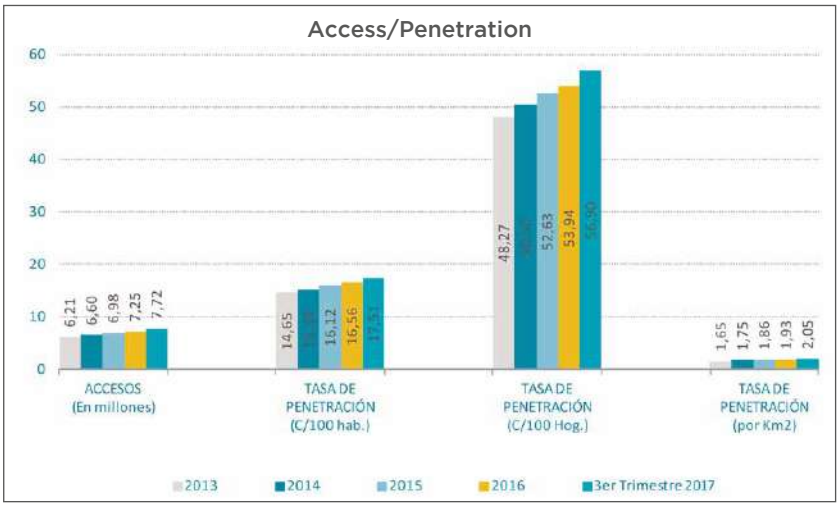
Likewise, in relation to access and penetration related to the fixed Internet access service, it can be observed that between 2015 and 2017, 740,000 new accesses were generated, which increased the service penetration rate accordingly:

	2015	2016	3rd Quarter 2017
ACCESS (In millions)	6,985	7,252	7,725 [1*]
PENETRATION RATE (C/100 hab.)	16.12	16.56	17/51

[1*] A total of 113 new providers have been added to the list.

	2015	2016	3rd Quarter 2017
PENETRATION RATE (C/100 Hog.)	52-63	53,94	56.90
PENETRATION RATE (per km²)	1.86	1.93	2.05

Source: ENACOM



Source: ENACOM

Regarding technology access in this service, the deployment of Fiber to the Home (FTTH) has increased, considering that in 2015 there were approximately 139 thousand accesses and in 2017, 194 thousand accesses were surveyed using this means, accounting for an increase of 40%.

Finally, in the international context, and in a global evaluation, it can be observed through the ITU ICTs Development Index (IDI)[74], the evolution since 2015 with an IDI = 6.40 at 2017 with an IDI = 6.79, which places Argentina at # 51 in the world ranking.

74 IDI (ITU): <http://www.itu.int/net4/ITU-D/idi/2017/index.html>.

6.2 Analysis

The question about the deployment and development of Telecommunications Infrastructure can be divided into two main situations:

- Deployment of infrastructure in neglected areas, typically rural areas.
- Development of the existing infrastructure in connected areas, typically urban and sub-urban.

In the case of Argentina, it is necessary to consider that it is a large country in terms of area, and achieving full coverage of its territory is a demanding challenge. It is for this reason that these challenges must be addressed by the development of public policies with a plan that includes measures in the short, medium and long term.

Given that this is not an isolated problem in each country, Argentina participates actively in the areas of discussion that address these issues.

In this sense, Argentina is part of the Internet for All program[75], morganized by the WEF (World Economic Forum), the Working Party on Communication Infrastructures and Services Policy (WCISP) of the Committee on Digital Economy Policy (CDEP)[76] of the OECD and the work spaces within the International Union of Telecommunications Development Sector (ITU-D)[77], this last area in which Argentina hosted the last World Telecommunication Development Conference (WTDC-17)[78].

6.3 Deploying infrastructure in neglected areas

There are great geographical difficulties for deployment in neglected areas, because they generally correspond to rural areas, remote places and areas of difficult access. But certain bureaucratic, tax and regulatory obstacles or barriers that hinder the deployment of infrastructure are also identified, such as:

75 Internet For All (WEF): <https://www.weforum.org/projects/internet-for-all>.

76 Committee on Digital Economy Policy (CDEP): <https://oecdgroups.oecd.org/Bodies/ShowBodyView.aspx?BodyID=1837&Book=True>.

77 ITU-D: <https://www.itu.int/en/ITU-D/Pages/default.aspx>.

78 CMDT-17 (ITU-D): <https://www.itu.int/en/ITU-D/Conferences/WTDC/WTDC17/Pages/default.aspx>.

- High costs related to the civil works required for the deployment of fiber optic, currently considered the most appropriate physical medium to perform access networks, backbone networks and the links that connect both networks (backhaul).
- High costs related to spectrum access. In this sense, the private sector is considering other alternatives to auctions, such as, for example, the Beauty Contest modality for Spectrum Adjudication Contests, arguing that by lowering entry costs, a reduction in end user prices would be achieved.

On the other hand, the key role of the contributions related to the Universal Service obligations in the deployment of Telecommunications Infrastructure is highlighted.

6.4 Development of the existing infrastructure in connected areas

In relation to the areas that already have access to services, typically urban and sub-urban areas, the need to continue developing the existing infrastructure is recognized, because the new applications and services generate a growing demand for infrastructure resources to give supply to the increase in data traffic. This situation means that some services, which have service coverage, experience a lack of resource capacity, which does not allow providing the service according to the defined parameters of Quality of Service (QoS).

Among the difficulties that have been analyzed, the following stand out:

- Lack of development of access networks and penetration of transport networks (backbone).
- Municipal regulations that interfere in the deployment of the Telecommunications Infrastructure, either through taxes (such as rights of way) or restrictive requirements on civil works (such as the bearing structures of the irradiating systems).
- Availability of radio spectrum for use in access networks that can meet the demands of capacity.

These difficulties are addressed as a whole and the Public Policies section will mention the different measures implemented with the aim of resolving them.

6.5 New technology and regulatory trends

Trends and the evolution of technology currently generate a wide range for specific solutions according to needs, which include solutions with infrastructure using wired physical media (fiber optic, coax cable, etc.) or wireless (terrestrial or satellite links).

Within the framework of the OECD's CISP Working Group, for example, new technological and regulatory trends have been analyzed and debated, which make up connectivity solutions that make it possible to reduce the digital divide in rural areas.

Among the ideas under discussion is to facilitate access to passive infrastructure (poles and pipelines) by reducing deployment costs, promoting open access networks with public funds to optimize deployment investment plans, stimulate community network initiatives at the municipal level to reduce the cost of providing broadband in the networks of access, reuse the existing infrastructure in order to reduce costs and redundancies and encourage the deployment of services in remote areas through competitive and transparent tenders through loans with reduced interest rates, subsidies or tax exemptions.

In strictly technological terms, in relation to the evolution of standards, the importance of the deployment of fiber optic networks for transport networks (backbone and backhaul) is recognized.

On the other hand, copper networks, which take advantage of fixed public telephone lines and use xDSL technologies, have evolved with the VDSL2 standard, while the highest speeds on these networks are achieved with the G. Fast standard. On the other hand, the coaxial networks of the cable operators implement hybrid HFC (Hybrid Fiber-Coaxil) networks using DOCSIS standards.

Regarding wireless technologies, evolutions are observed in those related to LAN coverage (Local Area Network), which are mainly

developed by the IEEE (Institute of Electrical and Electronics Engineers), such as the IEEE 802.11ac and IEEE 802.11ad standards. In relation to the 4G mobile technologies such as LTE (Long Term Evolution) of the 3GPP (3rd Generation Partnership Project), the 5G technologies will be added, which will meet the most advanced technical requirements of their previous generation, according to the Report ITU-R M.2410 "Minimum requirements related to technical performance for IMT-2020 radio interface (s)"[79], such as user data speed, latency, spectral efficiency and mobility.

Among the specific technologies for Internet of Things applications (IoT) standards such as LTE-M, NB-IoT, Sigfox and LoRa, among others, are available. These standards are generally characterized by their low power consumption (the devices can be powered by batteries or batteries with a duration of years), low data rates and the ability to share the resources of the access network simultaneously (using variants of Wider Spectrum, for example).

It also recognizes the existence of innovative projects in the field of satellite services, such as new satellite constellations formed by a network of hundreds of satellites, LEO (Low-Earth Orbit) or MEO (Medium-Earth Orbit) for the provision of data services Broadband with connectivity objectives in remote or rural areas, such as the OneWeb Project[80]. With respect to geostationary satellites (GEO), there are High Throughput Satellite Systems (HTS) which use multiple spot-type beams to increase the efficiency of spectrum reuse and thus increase the system's transfer capacity.

There are innovative projects, such as the Loon Project[81] Driven by Google or the Drones Deployment Project, also called UAV (Unmanned Aerial Vehicle), such as the Aquila[82] developed by Facebook or the Zephyr drone[83] manufactured by Airbus, which share the objective of providing connectivity services in rural and remote areas.

79 See <https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2410-2017-PDF-E.pdf>.

80 See <http://www.oneweb.world/>.

81 See <https://x.company/intl/es-419_en/loon/>.

82 See <https://www.facebook.com/notes/mark-zuckerberg/the-technology-behind-aquila/10153916136506634/>.

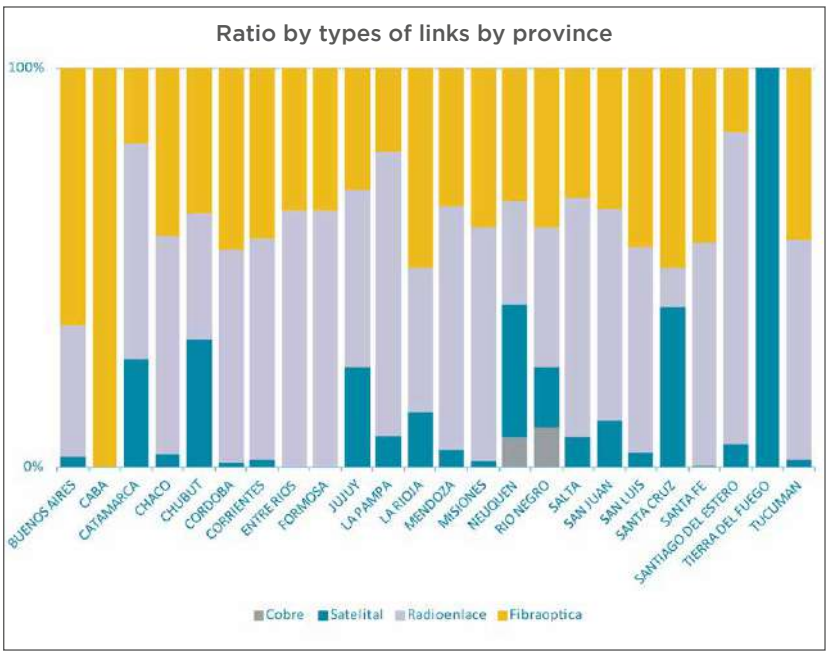
83 See <http://defence.airbus.com/portfolio/uav/zephyr/>.

6.6 Infrastructure in Argentina

An essential aspect for the analysis and planning of infrastructure development is to establish the current state of the deployment of the same at the national level. In this sense, ENACOM has implemented a web portal (https://indicadores.enacom.gob.ar/) with indicators and statistics related to telecommunications services.

Below, some current data on telecommunications infrastructure is reproduced[84] and Internet access[85] in Argentina, relieved with the information provided by the telecommunications services providers according to local regulations.

- Proportion of physical links displayed by province:

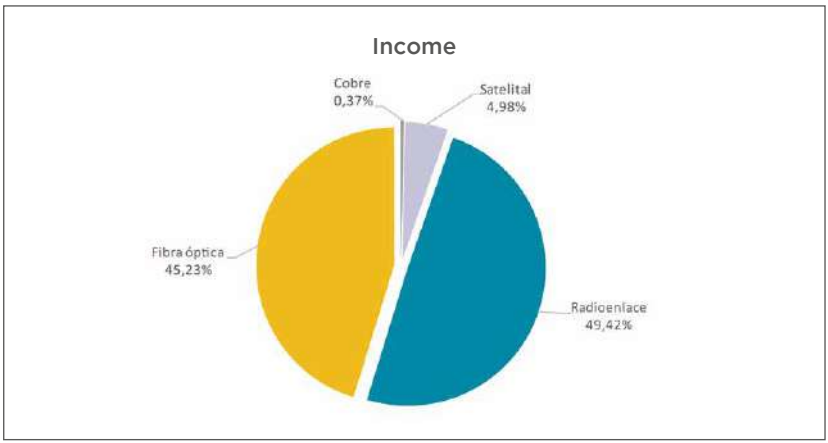


Source: ENACOM

84 Market Report – Infrastructure – 3rd quarter 2017 (ENACOM): <https://www.enacom. gob.ar/multimedia/noticias/archivos/201712/archivo_20171211074400_1011.pdf>.

85 Market Indicators – Internet Access – 3rd quarter 2017 (ENACOM): <https://www.enacom.gob.ar/multimedia/noticias/archivos/201712/archivo_20171211074252_4575.pdf>.

- Proportion of types of links used:

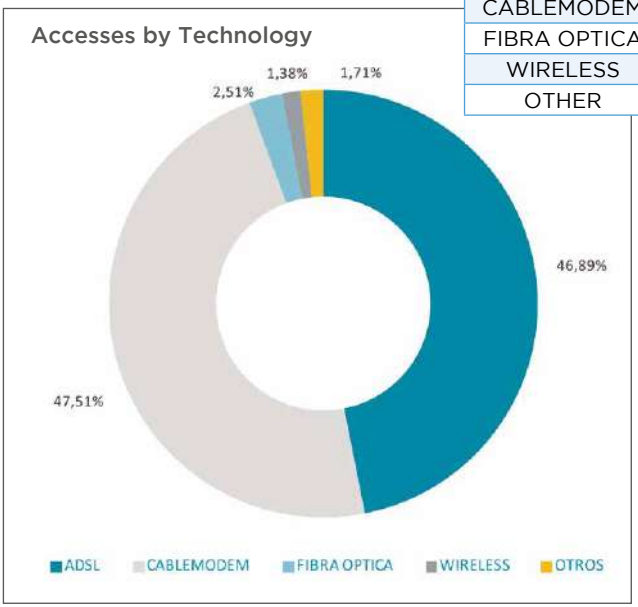


Source: ENACOM

Regarding the total of trunk links, there is evidence of greater investment in fiber optic lines.

- Fixed Internet access disaggregated by technology.

TECHNOLOGY	ACCESS
ADSL	3,622,575
CABLEMODEM	3,670,221
FIBRA OPTICA	193,964
WIRELESS	106,443
OTHER	131,740



Source: ENACOM

- Fixed Internet access statistics:

	Access (In millions)	Penetrarion Rate (C/100 Inhabitants	% of the Population with Internet access	Penetrarion Rate (C/100 homes)	% of the Households with Internet
3rd Quarter 2017	7,725	17,51	17,51%	56,90	56,90%

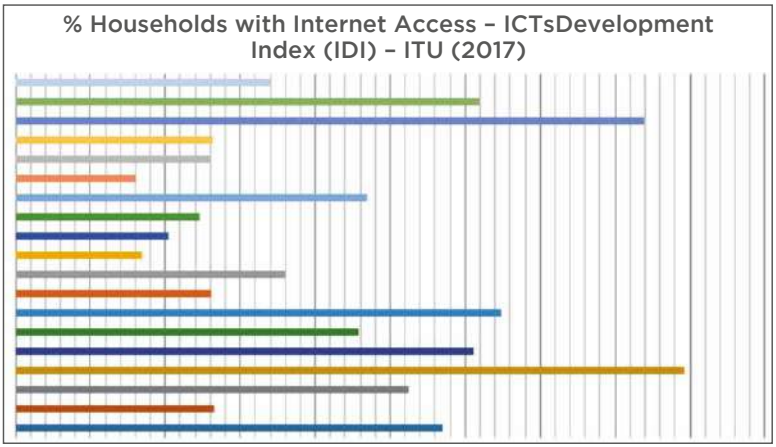
	Broadband Access (In Millions)	Broadband Penetrarion Rate (C/100 Inhabitants	% of Population with access to Broadband Internet	Broadband Penetrarion Rate (C/10 homes)	% of the Households with Broadband Internet access
	7,697	17,44	17,44%	56,69	56,69%

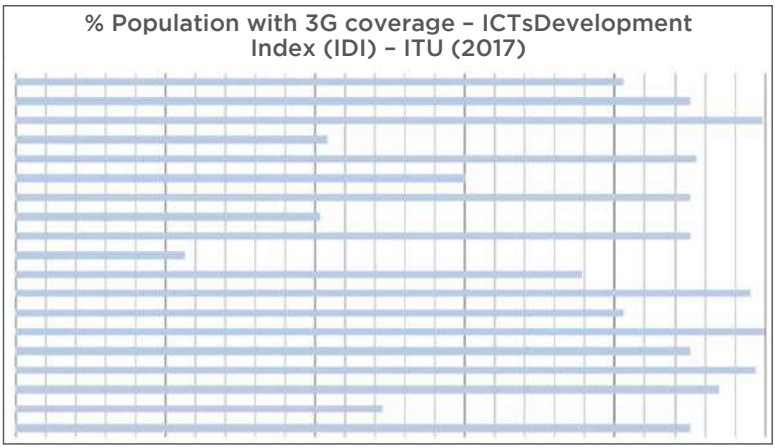
Inclusive Dial Up e Broadband over power lines (BPL)

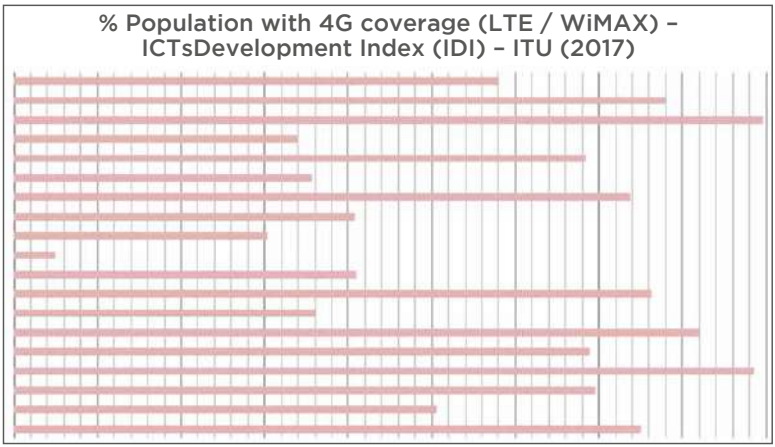
ADSL	CABLE MODEM	FIBER OPTICS	WIRELESS	OTHERS
3.622.575	3.670.221	193.964	106.443	131.740
46,89%	47,51%	2,51%	1,38%	1,71%

Source: ENACOM

- In the regional context, the percentage of households with Internet access relieved by ENACOM can be compared with the same indicator identified by ITU (2017) for the countries of the Americas, as well as the percentage of population with service coverage with 3G and 4G technologies:







6.7 Public Policies and Regulation

Based on the analysis of the situation and considering the points of view of the actors involved in telecommunications, measures were developed to encourage and favor the development of the Telecommunications Infrastructure:

6.7.1 Universal service

A new General Regulation of Universal Service was created[86] with the aim of contemplating the new scenarios and implementing an agile system to carry out the management of the programs.

86 Resolution 2642 ENACOM / 2016: <https://www.enacom.gob.ar/multimedia/normativas/2016/Resolution-2642_16-ENACOM.pdf>.

The Universal Service programs include, among others, the provision of ICT Services to groups of users with special needs who have access limitations to them, connectivity for public institutions, the modernization of service networks of Cooperatives and SMEs and the connectivity to the Natinal Fibert Optic Network (REFEFO) by telecommunications /ICTs licenses.

6.7.2 Connectivity Program

The Connectivity Program[87] promotes the implementation of projects for the provision of wholesale or retail services in areas with unmet needs, through the development of transport and access networks. In relation to the Connectivity Program, a Project for Access to ICTs Services has been approved through REFEFO[88] so that the public operator ARSAT generates the necessary conditions to access this network of all licensees of ICT Services, within the framework of the Federal Internet Plan[89].

In relation to this Project, Resolution 5410 ENACOM / 2016 established the commissioning of 120 distribution nodes of the REFEFO, being implemented with the Universal Service Trust Fund for a total amount of $ 1,329,000,000 to allow connectivity, together with the pre-existing network deployment, reaching a total of 890 localities, whith a total of approximately 15 million inhabitants.

Subsequently, through Resolution 5918 ENACOM / 2017, the development of 550 additional distribution nodes is planned, with the sum of $ 2,928,173,500 from the Universal Service Trust Fund being allocated for this second stage, with the objective of reaching locations between 100 and 5000 inhabitants. A relevant measure was to establish the terms and conditions for the provision of wholesale services in this project. In relation to this, connectivity and Internet access will be guaranteed by ARSAT in such a way that this price will not exceed USD 23 per Mbps capacity. This

87 Resolution 3597 ENACOM / 2016: <https://www.enacom.gob.ar/multimedia/normativas/2016/Resolution-3597_16-ENACOM.pdf>.

88 Resolution 5410 ENACOM / 2016 and Resolution 5918 ENACOM / 2017: <https://www.enacom.gob.ar/multimedia/normativas/2016/Resolucion-5410_16-ENACOM.pdf>, <https://www.enacom.gob.ar/multimedia/normativas/2017/res5918%20(December).pdf>.

89 Federal Internet Plan: <https://www.argentina.gob.ar/comunicaciones/planfederaldeinternet>.

measure has managed to abruptly lower wholesale capacity costs related to data transport and Internet access[90].

On the other hand, there have been calls for tenders, also within the Connectivity Program, like the call established in Resolution 8955 ENACOM/2016[91] which aims to implement projects for the universalization and improvement of network infrastructure for Internet Access in areas with unsatisfied needs.

In this call for projects, a partial financing through non-reimbursable contributions is granted, totaling up to $ 350,000,000. On the other hand, the projects must be framed in localities of up to 2500 inhabitants for providing ICTs services (except where there is already another service provider) or localities of up to 500 inhabitants without Internet access service.

Currently, six projects have been approved to Cooperatives and SMEs. The localities reached are in the provinces of Córdoba, Jujuy, Mendoza and Río Negro and a total of approximately $ 7,500,000 are distributed among these projects as non-reimbursable contributions.

6.7.3 Digital Education Networks Program

The Digital Education Networks Program[92] objective is to develop the internal network infrastructure of state educational establishments for the use of broadband internet access services, favoring educational practices and training processes.

It should be noted that the program is implemented through the execution of projects whose presentation is carried out by EDUC. AR, with the intervention of the Ministry of Education and Sports, while ENACOM, as the Application Authority of the Universal Service Trust Fund, receives the projects and evaluates them for its eventual implementation.

---

90 Newspaper article: ARSAT reduced the average cost of the Mega wholesaler by 50% – (01/19/2017). *The Daily Economist:* <http://www.eleconomista.com.ar/2017-01-arsat-redujo-50-el-costo-promedio-del-mega-wholesaler/>.

91 Resolution 8955 ENACOM / 2016: <https://www.enacom.gob.ar/multimedia/normativas/2016/res8955.pdf>.

92 Resolution 1035 ENACOM / 2017: <https://www.enacom.gob.ar/multimedia/normativas/2017/res1035.pdf>.

In May 2017, a project was approved for the development of the internal network infrastructure in 18,320 properties corresponding to state-run educational establishments. The approved budget for this project was up to $ 2,300 million and in July 2017, $ 600 million was disbursed to EDUC.AR as an advance.

6.7.4 Obligations to deploy fiber optic infrastructure in infrastructure works

In Decree 798/2016[93], it is established that the agencies of the National Administration, Companies and State Companies, among others, will eventually have in their infrastructure works that involve channeling, laying of poles or conduits, the obligation for laying of fiber optic networks.

This facilitates the implementation, lowering the costs of civil works that mean a difficulty for their development.

6.7.5 Municipal Regulations

As demonstrated by operators, in particular those of the mobile service, in relation to regulations Municipalities interfere with the deployment of infrastructure. ENACOM has promoted dialogue with different Municipalities in order to promote the adoption of a Model Municipal Regulation related with the installation of support structures for irradiating systems (masts / towers / etc.).

It is important to emphasize that the installation of an antenna support structure requires compliance with the regulation referring to the civil work involved, which is a Municipal competence. In addition, an agreement was made with the Secretary of Municipal Affairs (SAM) with the aim of providing training and technology in those municipalities that request it[94].

6.7.6 New Technologies

In relation to technological and regulatory trends, a Framework Agreement of Cooperation and Technological Assistance has been

93 Decree 798/2016: <https://www.enacom.gob.ar/multimedia/normativas/2016/ Decree-798_2016.pdf>.

94 ENACOM and SAM Convention: <https://www.enacom.gob.ar/institucional/conectando-municipios_ n1701>.

made between ENACOM and Microsoft of Argentina[95] to exchange information related to new technologies, as well as to promote implementation evaluations, among other aspects.

This agreement will allow testing of connectivity with technologies that optimize the use of unused radio spectrum, such as Dynamic Spectrum Access Systems through the use of Cognitive Radio, such as radio interfaces that implement the IEEE 802.22 standard. Said technological standard allows to detect channels of the UHF TV band that are free (called Blank Spaces) and use them to transmit data.

6.7.7 Community Network

Community Networks are networks built and generally operated by people from the community where they are deployed, performing the operation of the non-profit network in areas where there is normally no Internet access. In order to promote them, ENACOM signed a Memorandum of Understanding with the NGO Internet Society[96], which will allow cooperating with each other to strengthen the social function of the Internet and the implementation of policies on infrastructure deployment related to Community Networks, pursuing the goal of achieving Internet access in numerous communities.

6.7.8 Deployment of Wi-Fi Access Networks

There are several initiatives developed by the public sector related to the deployment of free Wi-Fi networks in public areas such as plazas, transport stations, libraries and hospitals, and so on.

Just to cite some initiatives:

- Information Highway, which currently implements 1,179 access points in the province of San Luis and is driven by the Government of said province[97].
- BA Wi-Fi network (which recently added 150 new access points reaching 563 points in total) and is developed by the Government of the City of Buenos Aires[98].

95 ENACOM Cooperation Agreement – Microsoft: <https://www.enacom.gob.ar/institucional/enacom-sign-an-agreement-with-microsoft_n1326>.

96 Memorandum of Understanding ENACOM – ISOC: <http://portal.isoc.org/isoc/revista-isoc-October.pdf>.

97 See <http://wifi.sanluis.gov.ar>.

98 See <http://www.buenosaires.gob.ar/noticias/ba-wifi-sumo-150-nuevos-puntos-de-acceso-en-spaces-al-aire-libre>.

6.7.9 Passive and Active Infrastructure Sharing

The Infrastructure Sharing can be classified as:

- **Passive Infrastructure Sharing:** co-location or other modalities of sharing facilities, including ducts, buildings or towers (Directive 2002/19 / EC[99]). In this way, the passive infrastructure includes all elements of civil engineering and non-electronic infrastructure, such as physical sites, poles, masts, conduits, rights of way, generators, air conditioning equipment, battery, power supply, and so on.
- **Active Infrastructure Sharing:** Provision of specific services and active network elements necessary for ensure users interoperability of end-to-end services, including facilities for intelligent network services or roaming in mobile networks (Directive 2002/19 / EC). According to the previous definition, the active infrastructure includes all the electronic elements of the telecommunications infrastructure, such as the network access management equipment, the base stations of the mobile service, the optical network units (ONU), multiplexing equipment, etc.

In the local regulations, Resolution 4510 ENACOM / 2017 incorporates specific active and passive infrastructure sharing definitions for the Advanced Mobile Communications Services (SCMA)[100], which are the mobile services provided with 4G (or higher) technologies:

- **Passive Infrastructure Sharing:** is the shared use of physical space, energy, network support infrastructure and other telecommunications infrastructure facilities.
- **Active Infrastructure Sharing:** is the shared use of active elements that make up the access, transport and/or switching network for mobile communications.

These tools facilitate the deployment of Infrastructure both in connected areas or cities through the passive infrastructure sharing, which expedites access to support infrastructure, such as sites with mobile base stations, as well as in rural areas or

99 Directive 2002/19 / EC of the European Parliament and of the Council: <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32002L0019&from=ES>.

100 Resolution 4510 ENACOM / 2017: <https://www.enacom.gob.ar/multimedia/normativas/2017/res4510.pdf>.

unattended through the sharing of active infrastructure, in which two or more operators can be associated for a single deployment of access and transport network (*backhaul*) dividing costs into areas that individually are not profitable.

In relation to the Public Contest for the awarding of frequency bands of the mobile service carried out according to Resolution 38 SC / 2014, it was defined in the General and Particular Terms and Conditions[101]. Passive Infrastructure Sharing Obligations among the awardees.

In addition, Resolution 4656-E/2017 ENACOM defines a Model "Authorization Agreement for the Sharing of Active and/or Passive Infrastructure, Automatic Itinerancy and Service Goals"[102] to be entered into among the current SCMA providers that were awarded the aforementioned tender.

On the other hand, and in a specific relation to the passive infrastructure sharing among mobile service providers, Decree 798/2016 instructed the State Assets Administration Agency (AABE for its name in Spanish) to carry out the procedures that allow granting the onerous use of installations or real estate sector of the National State that are apt for the installation of antennas bearing structures.

Finally, Decree 1060/2017[103] establishes that the bodies of the National Administration, Companies and State Societies must guarantee to ICT service providers and independent operators of passive infrastructure, multiple or shared access, for a fee, to passive infrastructures suitable for the deployment of networks.

More information on this topic can be found in the ITU Report – "Six degrees of sharing" (2008)[104], which details the actions taken by governments, operators and service providers related to the sharing of passive and active infrastructure.

---

101 Resolution 38 SC / 2014: <https://www.enacom.gob.ar/multimedia/normativas/2014/Resolution-38_14.pdf>.

102 Resolution 4656 ENACOM / 2017: <https://www.enacom.gob.ar/multimedia/normativas/2017/res4656.pdf>.

103 Decree 1060/2017: <https://www.enacom.gob.ar/multimedia/normativas/2017/Decreto-1060_17.pdf>.

104 ITU report "Six levels of sharing" (2008): <https://www.itu.int/pub/D-PREF-TTR>.This summary was last updated in 10-2008>.

6.7.10 Spectrum management

6.7.10.1 Mobile Virtual Network Operator (MVNO)

In 2016, the former Ministry of Communications developed a new MVNO Regulation[105] which regulates the provision of mobile broadband voice and data services through MVNOs, increasing competition in the market and allowing companies that do not have their own spectrum and infrastructure the possibility of providing said services.

Currently, more than 10 MVNO registrations have been granted to licensees of ICT Services. Regarding the agreements between real operators and MVNOs, the one made by CATEL (Chamber of Telecommunications Cooperatives) with Telefónica Móviles Argentina (Movistar) stands out[106].

CATEL informs that, acting as MVNO, it will provide mobile telephony in the provinces of Buenos Aires, Cordoba, Santa Fe, La Pampa, Mendoza, Misiones, Chubut, Rio Negro and Santa Cruz through the associated cooperatives, which may package the offers of services adding Fixed Telephony, Internet Access and Television.

6.7.10.2 Spectrum for Mobile Services (2G / 3G / 4G technologies)

Radio resources for the provision of mobile services are a key aspect for the development of these services, given the growing demand generated by this resource for the permanent increase in data traffic. In this regard, the allocation of new bands and a mechanism were implemented to facilitate access to the spectrum, through a procedure that allows the reuse of frequency bands initially identified for other services: a tool known as refarming.

New attributions to the SCMA: Through Resolution 1033 ENACOM / 2017[107] and Resolution 1034 ENACOM / 2017[108], the 2.6 GHz band

105 Resolution 38 MINCOM / 2016: <https://www.enacom.gob.ar/multimedia/normativas/2016/Resolution-38_16-MINCOM.pdf>.

106 Agreement between CATEL and Telefónica Móviles Argentina: <http://catel.org.ar/telefonica-y-catel-theysigned-an-agreement-that-will-allow-to-the-cooperatives-to-render-services-of-mobile-telephone-in-different-areas-of-the-country/>.

107 Resolution 1033 ENACOM / 2017: <https://www.enacom.gob.ar/multimedia/normativas/2017/res1033.pdf>.

108 Resolution 1034 ENACOM / 2017: <https://www.enacom.gob.ar/multimedia/normativas/2017/res1034.pdf>.

and a segment of the 900 MHz frequency band, respectively, were allocated to the Mobile Service.

In this way, a total amount of **580 MHz** available to Mobile Services that are implemented with 2G / 3G / 4G technologies (called by the ITU "IMT Systems", International Mobile Telecommunications Systems), being Argentina one of the countries in Latin America with the largest amount of spectrum attributed to this service.

Refarming procedure: Resolution 171 MINCOM / 2017[109] establishes the regulation of Refarming, which aims to regulate the process aimed at releasing, in whole or in part, the assignments of existing frequencies in a certain frequency band, originally assigned to certain services, to then be those frequencies attributed to the same service or different services of greater spectral performance and latest technological generation.

Through this Refarming tool, the project was approved for a provider to provide SCMA in the 900 MHz and 2.6 GHz bands[110], while the remaining frequency segments of the 2.6 GHz band were offered under a Spectrum Assignment on Demand procedure[111] among the three incumbent providers of Mobile Services in Argentina.

As a result of the new spectrum allocated and awarded, through the processes of Refarming and Spectrum Allocation on Demand, the providers have been left with the following amount of spectrum for mobile services with 2G / 3G / 4G technologies:

Provider	Mobile Services Spectrum Quantity [MHz]
Telecom Personal (Personal)	140
Telefónica Móviles Argentina (Movistar)	120

109 Resolution 171 MINCOM / 2017: <https://www.enacom.gob.ar/multimedia/normativas/2017/res171M.pdf>.

110 Resolution 1299 ENACOM / 2017 and Resolution 3909 ENACOM / 2017: <https://www.enacom.gob.ar/multimedia/normativas/2017/res1299.pdf>, <https://www.enacom.gob.ar/multimedia/normativas/2017/res3909.pdf>.

111 Resolution 3687 ENACOM / 2017: <https://www.enacom.gob.ar/multimedia/normativas/2017/res3687.pdf>.

Provider	Mobile Services Spectrum Quantity [MHz]
AMX Argentina (Claro)	130
Nextel Communications Argentina (Nextel) (*)	80

(*) Note: The Telecom Personal and Nextel providers are in the process of merging. From ENACOM, through Resolution 5644 ENACOM / 2017[112], this process was approved with certain obligations, including the elaboration of a frequency return proposal because the amount of spectrum.The radio spectrum of both providers exceeds the spectrum cap (140 MHz), in order to comply with said ceiling, defined in Resolution 171 MINCOM / 2017.

This amount of spectrum per operator is comparable to that of providers in developed markets for the provision of Mobile Services with 2G / 3G / 4G technologies, such as:

- Italy: Telecom Italia (165 MHz)
- Spain: Vodafone Spain (175 MHz)
- Switzerland: Salt Mobile (formerly Orange Network SA) (160 MHz)
- Sweden: HI3G Access (145 MHz)
- United Kingdom: Telefónica UK (100 MHz)

This information is transcribed updated to December 2017 and is available in Report 03 of the European Communications Office (ECO) "The licensing of 'Mobile Bands' in CEPT[113]" (CEPT, European Conference of Postal and Telecommunications).

Also, according to the information provided by All net Insights & Analytics, a company dedicated to the study, analysis and preparation of reports and tools related to the radio spectrum in the USA and published on the website of the company Fierce Wireless[114], the providers of Mobile Services in the USA count to 2017, also with comparable amounts of spectrum:

112 Resolution 5644 ENACOM / 2017: <https://www.enacom.gob.ar/multimedia/normativas/2017/res5644% 20(December).pdf>.

113 ECO Report 03 "The Licensing of 'Mobile Bands' In CEPT" (15/12/2017): <https://www.efis.dk/views2/report03.jsp>.

114 "In 2017, how much low-, mid- and high-band spectrum of Verizon, AT & T, T-Mobile, Sprint and Dish own, and where?" (FierceWireless): <https://www.fiercewireless.com/wireless/2017-how-much-low-mid-and-high-band-spectrum-do-verizon-at-tt-mobile-sprint-and-dish-own>.

- Verizon: 114 MHz
- AT & T: 178 MHz
- T-Mobile: 110 MHz
- Sprint: 202 MHz
- Dish: 93 MHz

Although in some localities there are still migration processes pending completion, in certain frequency bands, that hinders the total exploitation of the allocated spectrum, it is expected by all the measures adopted previously detailed, that the networks of the mobile services are developed, adopting new and more efficient technologies and improving the current Quality of Service (QoS).

Finally, it is worth mentioning that there is confusion in debates related with needs or barriers experienced by the industry or providers of broadband data services, the difficulty in the availability of the radio spectrum as a resource in rural or unattended areas when what happens is that the resource has high demand in urban areas where traffic reaches to congest the network, particularly at certain specific times and places, while spectrum resources are not scarce in rural or unattended areas, where for all the aforementioned, there is the availability of various regulatory tools (such as the sharing of active infrastructure, for example), technologies (such as that implemented in community networks in the 2.4 GHz and 5.8 GHz bands) and frequency bands (not only for mobile services with exclusive spectrum, but also frequency bands with shared mode) p to meet the needs required in terms of access to the radio spectrum to be used in access networks in these rural areas.

6.8 Conclusions

In the present article the main technology tendencies were exposed as well as the regulatory tools that favor their development. Likewise, the main difficulties expressed by different actors in the sector were stated and the regulatory measures and public policies implemented with the aim of resolving them were detailed.

As a result, the deployment of transport networks using fiber optics is a key aspect, as well as considering the main difficulties

related to the costs of civil works, and for this the management and administration of government tools is also fundamental, or mixed, that generate incentives such as, for example, Universal Service Funds.

Likewise, the deployment of the REFEFO not only managed to connect unattended locations but also allowed the promotion of competition, abruptly lowering the costs of transportation and Internet access wholesalers. Another relevant measure was the development of the new Regulation of the Universal Service Fund that allowed the financing of different projects, including a greater development of the REFEFO, in order to deploy Infrastructure and improve connectivity in specific areas.

Due to the importance of managing and making available more radio spectrum, particularly for mobile services, new regulations related to Refarming were implemented, as well as the allocation of the 2.6 GHz band and the demand allocation process of the same, allowing to satisfy the demands of spectrum in the medium term. To improve connectivity in rural areas agreements were made with companies and associations such as Microsoft and the Internet Society, for the implementation of new technologies and efficient models of access networks.

Finally, due to the dynamics of the sector, the importance of permanent dialogue between the public and private sectors is acknowledged, as well as participation and debate in international forums and organizations that allow exchanging information on best practices and evaluating case studies.

6.9 References

El Economista Diario. (2017). ARSAT redujo 50% el costo promedio del Mega mayorista. El Economista Diario. <http://www.eleconomista.com.ar/2017-01-arsat-redujo-50-el-costo-promedio-del-mega-mayorista/>.

Mike Dano (2017). In 2017, how much low-, mid- and high-band spectrum do Verizon, AT&T, T-Mobile, Sprint and Dish own, and where? Fierce Wireless. <https://www.fiercewireless.com/wireless/2017-how-much-low-mid-and-high- band-spectrum-do-verizon-at-t-t-mobile-sprint-and-dish-own>.

7 National and International Connectivity: the Case of IXP Buenos Aires Success

Oscar Messano

Abstract

Telling about a process that has been taking place for a little over 30 years in few pages is not a simple task. It is not a matter of placing proper names, and it would seem that one does not want to recognize the personal efforts of those involved in these years, never further from reality. Each and every one regardless of the size of their participation are responsible for the success of this project. As you will see, the participants are of varied national and international origins, NGOs, SMEs, governments, academia, incumbents, leading companies, among others, which makes this project an interesting laboratory for the creation and performance of the "multistakeholder" Model. Were all roses? No, there are always the thorns that are part of the challenges which come with any project, and avoiding them is part of any innovative activity. This chapter explores the success story of the IXP Buenos Aires, highlighting how today the project "Broadband Federalization" is in the process of growth and produces a permanent exchange of information with IXPs in the region. This has led to the creation of LAC-IX "The Association of Internet Exchange Points" ", a non-profit organization based in Uruguay, which gathers together ten countries with IXP in the region: Argentina, Brazil, Caribbean, Colombia, Costa Rica, Cuba, Ecuador and Paraguay.

7.1 Introduction

Usually, a project, whether social or commercial, does not happen spontaneously. There is always an initial environment that leads to the definition of actions to follow and develop the case project. Based on this premise is that I will present this successful case in historical contex, clarifying that it is a summary of 30 years of effort and dedication of a number of people made *ad honorem*.

In the 1980s, before the Internet became commercial, there were the so called value-added services: email, access to databases, telexes sending through data networks, among others. The cost of these services was high due to use of the technology of that time. In addition, the state had a communications monopoly and operated a packet network called Arpac[115]. This network invoiced based on time and packets (set of 64 bits) and despite these tariffs, a considerable traffic was produced. So which were the reasons for this traffic? Despite the tariffs, telex services, fax, access to databases through Arpac were cheaper than sending them through the telephone network and, on the other hand, the method of transmitting data through a computer was reliable and instantaneous. An industry of the telecommunications services, whether incipient, grew with a strong vision towards the future.

With the emergence of the Internet in 1995, the business model and the technological model began to change rapidly. At that time telecommunications had been privatized in Argentina and instead of a state own monopoly, it became a duopoly: two companies, one for the north part of the country and the other for the south. Both companies formed a third licensee focused on international telephony and international data services.

The incipient Internet service providers had to negotiate the bandwidth to provide Internet acess. The rate offered by the licensee was 40,000 US Dollars per month per 64 Kb. This fee made it impossible the use of the service. After a while the price dropped to 28,000 US Dollars per month and consequently each provider had to negotiate the best rate they could obtain.

In any case, the growth in bandwidth and number of customers was slow and practically not sustainable.

Let's go back a bit to the past, to the time of ENTEL (National Telecommunications Company). In order to have a relevant dialogue channel with ENTEL, the Argentine Chamber of Databases and Online Services CABASE, was created in 1985. Its six founding partners have grown since then to 80.

115 ENTEL data network (National Telephone Company)

7.2 The Internet arrival

Given the new market conditions, the suppliers associated with the CABASE began to design what then would be called the NAP *Network Access Point*. The idea was that the creation of a single point contact for interconnection and the joint purchase of a greater bandwidth would bring a substantial decrease in costs, adding the benefits of fixed costs sharing such as energy, UPS, security, common expenses, technical and administration aspects. These all represented an important competitive advantage, which meant a substantial improvement for all associated companies. This model was also attractive for incumbents and large operators such as Telefónica and Telcom as well as Impsat, Comsat, Clarín, among others. This was the first step towards a project that would be successful and recognized worldwide.

The project was not easy to implement, achieving consensus in companies that are normally competitors was not an easy task. It was the beginning of the understanding that the Internet was a new communications technology and also a new vision for trading and social change. Finally, the vision of a promising future of the sector led to the unification and consensus of the participants.

In 1998, Argentina´s first NAP was inaugurated by the former National Telecommunications Commission´s Deputy Controller, which supported the project. This project was the first demonstration of what would later be called the "multistakeholder model". This association was founded by 12 CABASE's Internet service provider partners, the Government's National Telecommunications Commission, several companies (SMEs, incumbents, etc.) and the industry associations.

They were years of permanent growth of traffic and services[116] increased bandwidth thanks to the low cost of Mb benefiting users with better Internet services, but this was circumscribed to Buenos Aires, leaving out these benefits to the rest of the country and mainly in areas of low population density locations, or economic level.

116 See the Observatory and Monitoring of CABASE in <http://www.cabase.org.ar/>.

The barriers for accessing the Internet were many. CABASE, decided to launch a new project called “Broadband Federalization”. Given the undoubted difficulties for the suppliers of the interior of the country for the provision of a good service and a reasonable and sustained growth, the objective was to generate the creation of other NAP in the interior of Argentina.

After a test made with suppliers from different provinces, it was agreed that the project´s pilot model would be carried out with the suppliers of the province of Neuquén. Once this decision was made, work began with the possible participants, and meetings gave information in order achieve a definition for this NAP. In Buenos Aires it was difficult making the service providers being aware that a collaborative effort represented advantages and that it was a win/win project. In the interior this was not very different, even though the specific experience of the NAP Buenos Aires already existed.

After more than a year of meetings, the first Interet traffic exchange point in the country´s interior was completed, including 8 service providers in its foundation.

In Buenos Aires the competitive advantages generated by the NAP were excellent, and in this first pilot of the the economic, logistical and commercial advantages were extraordinary. It was a witness case which was used for a long time as a success case: a service provider in San Martin de los Andes was paying $ 400 US Dollarsper Mbps, and after connecting to the NAP in Neuquén its cost per mega fell down to $ 54 US Dollars. With the monthly savings they deployed a microwave network project to connect San Martín de los Andes with Province Capital City Neuquén. Today there are two microwave networks and one fiber connecting another location. These figures do not require further comments.

It is interesting to note that there is no doubt that the main initial objective of the creation of a traffic exchange point (NAP) was the economic one. The differences in values supported this premise and over the course of time a number of direct or collateral technological benefits came to light and, as we will see later, the benefits to the user were assured.

7.3 The current situation

Moving forward in time, there are 27 operational IXPs today, named from the English *Internet Exchange Point*, and 4 more are under development. Originally the project had the objective of a NAP implementation in each province of Argentina. Then reality and the "need" changed this objective and as it is happening in some provinces, more than one IXP has been established.

Today these IXP are operational in Argentina:

	Province	City
1	Ciudad Autónoma de BsAs	
	Provincia de BsAs	
2		La Plata
3		Mar del Plata
4		Junín
5		Pergamino
6		Gran BsAs Zona Norte
7		Gran BsAs Zona Oeste
8		Tandil
9		Bahia Blanca
10		De La Costa
11	Neuquén	
12	Santa Fe	Santa Fe
13		Rosario
14	Mendoza	

	Province	City
15	Córdoba	
16	Posadas	
	Rio Negro	
17		Bariloche
18		Viedma
19	Puerto Madryn	
20	San Luis	
21	Tucumán	
	Chaco	
22		Saenz Peña
23		Resistencia
24	Jujuy	
25	San Juan	
26	Salta	
27	Rio Gallegos	

There is an old saying "Rome was not built in a day." This case is the same: they were years of constant work and it continues, keeping these 382 members of the association informed, providing administrative support, helping with logistics, technical issues, among others. It is the effort of the CABASE association which is rewarded by the constant growth of the system in a fluid and

constant relationship. Presently, more than 40 monthly video conferences are made.

Why is this a success story? These are the results of these almost 30 years of activity:

- 12 initial members growing to 382 at present
- 15 Mbps at the beginning to 600 Gbps at present
- value of the Mbps at the beginning 54 US Dollars (without counting the extreme case of 400 US Dollars)

Today there are three types of traffic:

a. IXP internal traffic among members of the IXP for free.

b. Traffic (national) between IXP 4/10 US Dollars

c. International traffic 14 US Dollars

Noteworthy is the participation of the following national agencies: AFIP (Federal Administration of Public Income), Province Bank, Gendarmerie, and Government of the City of Buenos Aires, National Judicial Power, Naval Prefecture, and the the academy. Particularly, with the networks of Innovared and Ariu, the academia actively participates in the network of IXP, and a significant amount of IXP are housed in University premises. This set of IXP interconnect 90% of Argentina's networks and gives access to approximately 13 millions of end users[117].

The high increase in traffic due to the permanent growth of services and applications on the Internet is constantly analyzed and monitored. It is concluded that the future bandwidth demand will be enormous and maintaining a quality service to the end user will be an important challenge for CABASE. This fact is essential to the strong discussion about network neutrality[118].

Among the measures designed to alleviate this problem there was the installation of a cache of the main CDN (*Content Delivery Network*). CABASE already supported for long-time company servers and organizations such as Verising, PCH, Nic .ar. In spite of this fact, the negotiation with the main content delivary players

117 CABASE – Observatory and Monitoring

118 See <http://www.networkneutrality.info/>.

started with the installation of the first Google Akamai and Netflix cache. Some of these are also found in the the IXP network.

There are a number of positive effects on the network, like lower costs of international connectivity as access to information is done on local servers, increased national connectivity, and a notable improvement of the end user in accessing content with a rational use of international bandwidth. In the beginning and as some may remember, a recurring theme was that an email addressed to a recipient 100 meters from the sender went to the United States and returned. In those days the Internet traffic in Argentina was 90% international and 10% national. Today the IXP network has 15% of international traffic and 85% of national traffic. This equation, additional to foreign currency savings, improves the end user´s quality of service.

Although this was initially developed in the IXP Buenos Aires (CABA), with the rapid increase in traffic within the IXP network, the installation of caches in IXP of the different provinces began to be replicated, improving costs and quality of service for the end users of these IXP. Today 16 of the 27 IXP already have local cache.

7.4 Conclusions

In conclusion, what began as a solution for the sustainability of suppliers and SMEs, allowed the creation of the first IXP in Latin America and contemporary with the first in the United States, which today is a tool for national social and technological development of the Internet. This is recognized worldwide as a Case of Success[119] and is replicated in other countries.

119 CABASE – Holds the presidency of LAC-IX. See <http://www.lac-ix.org/nosotros.html>.

8 Technological Evolution of Internet Pathways

Lacier Dias

Abstract

This paper explores issues related to Internet access in Latin America and the Caribbean, addressing the growing need to be connected, the impact that access has on the digital economy, and the lack of legal security for entrepreneurs and users who still persist in the region. To deal with these topics, the historical trajectory of physical infrastructure types, routing protocols and data routing technologies used in connectivity are initially discussed. In addition, the article also presents some perspectives for a future scenario, when dealing with the issue of the IPV6 implementation, the growth of community networks and the important role played by small and medium-sized suppliers. Finally, the article deals with the geographical, social and economic barriers faced by people dedicated to providing access to the network in the most diverse locations which are not covered by large commercial providers.

8.1 Introduction

The Internet is a universe that seems to be only technological, however, it is a world full of challenges. What is called technology or a more modern form of disruptive innovation is simply a term that points to the technological advances of products and / or services related to the Internet. This rupture occurs not because of an evolution, but because of the interruption of the existing technology, giving rise to other technological forms. It is the breaking of one process, which starts another, in a new way. And the pace of this disruption, in what refers to the technological advance of the Internet, has been increasingly faster by the demand of uninterrupted services and quality.

The Internet today is so present in social relationships, both professional or personal, that everyone wants to have it in the same way they have water or electricity services, which are always available. When a person arrives at a house or any other

environment, he knows that he will have access to water and electric power, except in some rare contingencies. In the same way, society as a whole wishes to have access to the internet: always free, without being hostage to connection instabilities.

The combination of greater demand for speed and stability, old services migrating to the Internet and the creation of new services exclusively online, have led to drastic changes in technologies over the past 20 years, both in the provision of Internet in companies and residences, as in the backbones that interconnect people to the services and contents that make this magical world of the Internet happen.

At the end of the 90s, there was basic dial-up Internet access in households, however, at the beginning of the 2000s, the installation of the first ADSL links began, even with few kilobits per second, it was no longer dependent on telephone lines and could be used 24 hours by paying a flat fee. The first steps towards broadband had been taken.

Telephony copper cables were, and still are, fundamental to the Internet, since most of the fixed broadband depends on those structures inherited from telephony with pairs of copper cables. However, we cannot forget the existence of coaxial cables for cable TV, satellite links and radio links, also known as wireless or wireless links, which have their share of responsibility in bringing the Internet to thousands of people. These technologies are not new, but they reinvented themselves to bring more and more broadband and services to users, even in the most inhospitable places.

Despite the considerable improvement in access, and that 50% of the Latin American and Caribbean population is already reached[120], disparities persist, especially in relation to the residential areas in developing countries, mainly in the less developed countries, broadband penetration remains low.

Even those with access to broadband tend to experience low download and upload speeds[121], which limits the activities on the internet.

120 See ITU (2016).

121 *Ibid.*

The report[122] of the United Nations Conference on Trade and Development (UNCTAD) indicated that the presence of the countries of Latin America and the Caribbean in the digital economy is still relatively limited. Along with Africa, the Latin American and Caribbean region has less than 2% of the digital companies in the world, with a market capitalization of more than one billion dollars in the last semester of 2017. The report also indicated that less than half of the countries in Latin America and the Caribbean have adopted data protection and privacy legislation, and less than a third of all Caribbean economies have consumer protection laws for online purchases.

This combination of lack of government understanding to create incentives, clearer rules and the need for investments to meet the continued growth of demand in the cities of higher consumption, such as Rio de Janeiro, Quito, Georgetown, Bogota, Montevideo, Mexico City, Buenos Aires, Caracas, Asunción, Paramaribo, San Salvador, among others of the Latin American and Caribbean region. Thus, it makes that, only in some neighborhoods, the population uses services with speeds higher than 10 Mbps, the majority of users, even in these large centers, use services with speeds below 10 Mbps, which is apparently the most commercialized speed in these regions. Even combining the old and new access technologies, there is another 50% of the Latin American and Caribbean region with no access to the Internet.

8.2 The Internet roads

Internet travels paths that the common consumer does not see: it is not clear how the Internet reaches their households. Basically, there are five most popular media types to bring the Internet to the consumer: twisted pair (the good old telephone cord), coaxial cables (the same used in cable TV connections), and radio links, satellite links and, the last incoming fiber optic.

They are different ways to carry data from one point to another. In the case of the twisted pair, it consist of two isolated strands of twisted copper, grouped and closed in a plastic coating. This is

122 See UNCTAD (2017).

the most popular and uses the technique called ADSL, a relatively old standard, but still very functional, which takes advantage of the fixed telephony infrastructure for Internet connection. There is also the coaxial cable, used in cable TV connections, also used to carry the Internet signal.

The coaxial cable is made by a copper central connector that transmits the signal surrounded by an insulating mesh, protecting the transmitted data and absorbing the interferences. Both are very popular in larger cities. However, there are radio frequency and satellite technologies. Satellite communication is an extreme case, as it is not very functional and, undoubtedly, the one with the worst cost-benefit ratio. However, radio frequency accesses, popularly known as wireless accesses, are responsible for digital inclusion in most of the poorest communities, large centers, and cities in the interior of Latin American and Caribbean countries. It does not depend on great physical infrastructure, they need low initial investment and they use little infrastructure in the clients. In these cases, those who live near the distribution center have a higher speed, while those who live far away have less. This is challenging.

The fiber optic is the only media that provides the same quality throughout the network, since this type of structure transports data signals as modulated light pulses and offers high capacity at high speed.

There are suppliers that mix the fiber, using it in the connections between the plants scattered around the city, using twisted pair cables, coaxial or radio link in the last mile which access the client, and very few but growing, that use fiber up to residence of the same end user.

The technological movement present in recent years focuses on replacing current access technologies that, although still used, have been migrating to a newer technology of greater capacity and quality like fiber optics.

The wired metal networks, which kicked off the Internet broadband process, are virtually non-existent in the cities of the interior, since radio connections predominate there. In the larger cities, there is a more accelerated substitution of current technologies by fiber

optic networks, although, until that substitution is made, residence by residence, company by company, society will have to coexist and reinvent a lot the current technologies. Like the routing protocols and data routing technologies, all those that have been used for more than 20 years, such as the *Border Gateway Protocol* (BGP), the *Open Shortest Path First* (OSPF) and the *Label Switching Multi-Protocol* (MPLS), all these technologies enhance the *backbone* which transports large volumes of data in a safe and functional way over many kilometers of network.

Although they already have some time in the market, the main and most disruptive protocols are the BGP and MPSL, which are present, or at least should, in practically 100% of the operations and have a range of resources of very high performance as *Virtual Routing and Forwarding* (VRF), *Pseudo Wire Emulation End to End* (PWE3) which allow elaborate traffic engineering strategies that today support the main *backbones* of the world.

8.3 Innovation, opportunities and challenges

It is important to highlight the emergence of technologies that are deploying and advancing at a rapid pace, such as *Software-Defined Networking* (SDN), a concept that promises to change the current scenario, and the Virtual Extensible LAN (VxLan) protocol that over the years can replace some existing implementations.

However, this growth can be slowed down by the lack of addresses. The IPv4 addresses, which are used today by 100% of the Internet, have been exhausted and its successor, IPv6 addresses, are being implemented at slow pace, slower than the speed that Internet users are activated.

This is a global problem, which has been announced for more than 20 years, and now the time has come when implementation is urgent and indispensable, as otherwise the Internet will collapse.

IPv6 is a protocol developed with improvements in terms of numbering resources and functionalities. However, it is totally incompatible with IPv4, which makes it necessary to have both protocols operating simultaneously, for that, among several options, there is a double stack or *dual stack*.

This feature, double stack or *dual stack*, is one of the forms of migration that has proven most efficient to support this implementation period, until all services and devices are compatible with IPv6 and IPv4 can be turned off.

However, a segment driven by challenges, not only technological, but geographic and social, is the challenge that drives disruptive technology. It is necessary to consider two elements in this enormous machine: the community networks that have a very important role in promoting digital literacy, and the development of local applications, services and contents and the enormous gear of regional suppliers[123] that even without government investment or financing from large economic groups, little by little, have been bringing the Internet network to the most remote Latin American and Caribbean cities, enabling companies and families that are more distant, geographically or socially distant to have similar services to those of large cities and urban centers.

The fundamental point is that technological innovations are not always possible due to a disruptive technology, but to a large extent, by disruptive people. That is, entrepreneurs, entrepreneurs and technicians involved in operations and teams dedicated to work and connectivity. They are actors who believe in the development of a region, however distant, from the effort and work of taking the Internet to the most remote places.

In 2001, computers were installed with a radio antenna for transmission over towers, which received signals via radio links from kilometers away. This was made to spread the Internet and take it to inhospitable localities.

From 2001 until to today, new equipment appeared in that universe and allowed the Internet entrepreneurs to little by little change poor stability devices with more robust equipment, better prepared and developed. This has improved the availability, since demand was slow offering more stable broadband to include new subscribers.

123 The term "regional provider" refers to companies that market the Internet in the same city, or several neighboring cities.

Although there are still locations that do not even know what an Internet signal is, it has been the responsibility of small entrepreneurs to take the networks to places that are difficult to access. These entrepreneurs have developed this market in the same way as the pioneers, who came during the colonial period in the the sixteenth century and entered the Latin American territories in search of material wealth, especially gold and silver.

These entrepreneurs are the ones who take care of the minimum infrastructure found in these locations, and even with all the adversities, they provide an excellent Internet service. It is thanks to the merit of small and medium-sized entrepreneurs that the Internet is growing by leaps and bounds on a large scale throughout Latin America and the Caribbean. What brings the Internet to unimaginable places is entrepreneurship and demand allied to the impulse given by the entry of new manufacturers with more accessible licenses and equipment, new ways of operating more efficiently, with scalability and service availability allied to entrepreneurship and demand, taking the Internet to unimaginable places.

It is a qualified job of innovative and enterprising people. Not only in disruptive technologies, but especially in those who accept the challenge of investing in a segment full of large economic conglomerates, complex regulations and, often, unclear rules. However, many agree to focus on the market in these more distant cities, investing time and financial resources to offer a product / service already widely used in large urban centers. Technology is fundamental, but without the entrepreneur, it will never reach these destinations.

8.4 Conclusion: Elephants, bees and individuals for a sustainable network

Large companies and organizations, whether governmental or not, are like elephants. They delay to move with great difficulty to do so. Each step is a complex movement. That is why the role of small and medium-sized entrepreneurs is important. The regional suppliers, on the contrary, are like bees, much more agile and efficient and, therefore, able to provide a service of a higher level than most of the giants of the industry.

In spite of the great difficulties, the countries have understood that it is important to invest in communication, and particularly in the Internet, in order to promote regional and national economic development. The investment does not necessarily have to be made in the big centers, but also in those corners outside the traditional commercial routes. In the end, the increase in the consumption of some services, increases as Internet access increases: mobile phones, tablets, laptops, among other items and secondary accessories. More than encouraging consumption, it forces manufacturers to develop new and different elements, creating the need to consume again.

Many large companies, some of the giants of the industry, have invested heavily in research and development of software and platforms to provide Internet access to people, in a comfortable and cheaper way.

However, for those who have access to a consistent and healthy development of the Internet, it is necessary to have a multistakeholder governance, with each sector, entity or institution playing its role in the vast universe of the global computer network. It is necessary to allign global rights and duties, with laws and constitutions of each country aiming towards a collaborative, transparent, multilateral and democratic Internet for all the users.

8.5 References

Bucco, R. (2018, 29 enero). Acesso a banda larga fixa cresce 7,15% em 2017, impulsionado por ISP. Telesíntese. <http://www.telesintese.com.br/acesso-banda-larga-fixa-cresce-715-em-2017-impulsionado-pelos-isps/>.

Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD) (2017). Information Economy Report. <http://unctad.org/en/PublicationsLibrary/ier2017_en.pdf>.

Unión Internacional de Telecomunicaciones (UIT) (2016).ICTsFacts and Figures 2016. <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf>

9 Broadband Infrastructure and Digital Inclusion in Brazil

Peter Knight

Note: this article is based on Knight P. (2016) *O Papel da Banda Larga no Desenvolvimento do Brasil*. In Knight, Feferman e Foditch (2016), *Banda Larga no Brasil. São Paulo: Novo Século*, pp. 13:53

Abstract

This chapter begins by presenting a statistical radiograph of the state of broadband Internet in Brazil: the evolution of its penetration from 2006 to 2016 (i.e. digital inclusion) and a comparison of this penetration and the prices of fixed and mobile broadband with other countries. The issue of quality of broadband service is also addressed. Below, some factors affecting the price of broadband in Brazil are analyzed, mainly extremely high taxation, which impacts the entire telecommunications sector, but also the degree of competition, the high costs of financing and installation of networks and the rental of infrastructure of other operators and the little investment of the public sector in networks. Federal public broadband policies are analyzed in Brazil, with emphasis on the development of the National Education and Research Network (RNP), the privatization of telecommunications since 1998, and the National Broadband Plan. The lack of effective priority of the federal and state governments in relation to the expansion of broadband and digital inclusion is highlighted. Finally, some conclusions are presented regarding the importance of holistic strategic planning for the use of information and communication technologies (ICT) and their analogical complements to accelerate the economic, social and political development of the country; the evolution of broadband in Brazil compared to other countries; and federal government programs for the expansion of broadband and digital inclusion.

9.1 Introduction

The universalization of high-speed broadband, high quality and low cost is fundamental to accelerate the economic, social and political development of Brazil. The country's competitiveness, within a globalized economy, depends more and more on knowledge and access to information. Broadband Internet is an essential infrastructure of the 21st century and enhances technological evolution in various areas, reducing costs and increasing the quality of services such as education, health and public safety, among others. Broadband can also strengthen the research and teaching system, promote innovation and economic development, contributing to a more just society and a more dynamic and competitive economy.

Extending fiber optic networks to almost all municipalities and, from these optical networks, building high capacity networks that reach the remotest remaining municipalities, should be one of the axes of a broader strategy for the use of information and communication technologies (ICT) in favor of the economic, social and political development of the country. It should be noted that, even when the user accesses the Internet through wireless technologies (fixed or mobile), it is necessary to have high capacity backhaul, via radio links to reach the fiber optic networks that are the backbones of the Internet.

Despite significant advances, broadband in Brazil is still slow, more expensive than it should be and often of inferior quality compared to other countries, as will be highlighted in the second section of that chapter. Within the country there are also great inequalities in access, quality and cost of broadband. It is essential to develop a broadband strategy for Brazil, as well as to give political priority to mobilize the necessary resources in order to remedy those deficiencies.

This chapter summarizes the current picture of broadband in Brazil compared to other countries and analyzes some of the main topics of the broadband public policy debate.

9.2 Current status of broadband in Brazil

Table 1 presents some data on Internet penetration and the capacity of access connections for the years 2006 – 2016[124]. These statistics show a progressive improvement in Internet access. However, in 2016 only 54% of households had access to any type of Internet connection and only 12% had a connection above 8 Mbps. Of individuals over 10 years of age, 61% accessed the Internet at least once a day in 2014. Among Internet users, 92% accessed it at home and 46% in transit.

Table 1 Broadband Internet Penetration, Brazil, 2006-2016.

Statistics / Year	2006	2008	2010	2013	2016
% private Households with Internet access.	15	20	27	43	54
% private households with Internet access with fixed broadband connection.	6	10	18	28	35
% private households with Internet access with mobile broadband connection (3G modem).	N/A	N/A	3	9	25
% private Households with Internet access with connection between 2 and 8 Mbps[a].	N/A	1	3	6	12
% private Households with Internet access with connection greater than 8 Mbps[b].	N/A	N/A	1	7	12
% of individuals over 10 years of age who accessed the Internet in the last 3 months before the investigation (classified as Internet users in the consultation).	28	38	41	51	61
% of Internet users with more than 10 years of age who accessed the Internet daily from any location.	13	21	25	36	86
% of individuals over 10 years of age who accessed the Internet in transit in the previous three months research at home.	N/A	N/A	N/A	N/A	92
% of individuals over 10 years of age who accessed the Internet in the three months prior to the investigation.	N/A	N/A	N/A	N/A	46

Source: CGI.br (2007-2017).
Notes: N/A not available
[a] Broadband is defined as 128 Kbps by Digital Subscriber Line (DSL), cable, radio or satellite.
[b] Transmission rates given only for addresses where the person who responded to the researcher knew the speed.

124 Access capacity refers to the maximum rate of transmission of information available between the end user and his connection provider. This depends on the technology used for this connection and may be asymmetric, with greater capacity to receive ("download") than to transmit ("upload").

The most detailed data for 2016 clearly shows that all these indicators are lower in rural areas, in poorer or remote regions (Northeast and North) and for individuals with lower income, education or social class. (CGI.BR, 2017, Tables A4, A5 A6 and C1, pages 324, 310-313, and 328).

For example, 98% of households in Class A had access to the Internet, but only 23% of households in classes D and E. And so on: 59% of urban Households vs. 26% of the rural population, 64% in the Southeast region vs. 40% in the Northeast, 95% of individuals with 16 to 24 years of age vs. 22% of those over 60 and 98% of people with higher education. 8% of illiterates or children's education had access to the Internet, according to the survey.

The same access differences by urban and rural areas, social class, large regions, age and education already existed from the beginning of these investigations in 2006, but all these indicators improved over time[125]. In summary, digital inclusion has advanced substantially, but much remains to be done to reach the poorest and/or least educated regions and individuals, the oldest age groups, and rural areas.

9.3 Comparisons: Brazil and selected countries

Brazil occupies unfavorable positions according to several indicators of Internet services compared to rich countries and other developing countries.

9.3.1 Internet penetration

Table 2 presents several indicators of Internet penetration in the selected countries. The first indicator is the fixed broadband penetration rate per 100 inhabitants. The rate of 11.5% places Brazil well below South Korea, in first place (38.8%), and also below most of the countries with a similar per capita income level (Uruguay, Russia, Argentina and Mexico). China, South Africa and India show penetration rates much lower than all other countries. In the case of India, it is because of the huge rural population, with low income level and instruction. South Africa faces many of the same

125 For more details, see Chapter 6. Knight, Feferman and Foditch (2016).

fixed broadband problems as Brazil, including little investment in infrastructure, little competition in the supply of fixed broadband services, and high connectivity costs.

Table 2 includes broader information technology indexes. These indices include: (a) the ICTs Development Index (IDI) of the International Telecommunications Union (ITU or International Telecommunications Union); (b) The IDI sub-index, which measures access to the network (IDI-Access); and (c) the Network Readiness Index (NRI) of the World Economic Forum. Regarding these broader indicators, among the BRICS Brazil is behind only Russia. In comparison with the three Latin American countries mentioned above, Brazil remains at the forefront of Mexico, at the same relative level of Argentina, but well behind Uruguay in the ranking of those respected international indices.

Table 2 Comparison of the classification of Brazil and selected countries in proportion to the population with fixed broadband, IDI, IDI Access Component, 2015 and NRI, 2015.

Country	Fixed Broadband (% of population) 2014[a]	IDI 2015 Ranking	IDA – Access 2015 Ranking	NRI 2015
Brazil	11.5	60	71	84
Russia	17.5	45	48	41
India	1.2	131	135	89
China	14.4	82	89	62
South Africa	3,2	88	88	75
Argentina	14,7	52	64	91
Mexico	11.6	95	98	69
Uruguay	24,6	49	50	46
South Korea	38.8	1	9	12

Sources: ITU (2015) for fixed broadband (p.222-225), IDI (Table 2.2, p.44) and IDI Access (Table 2.3, p.46), Dutta, Geiger & Lanvin (2015), Table 1 p. 8 for NRI.

Note: [a] Fixed broadband is defined as a connection greater than 256 Kbps download via DSL, coaxial cable, FTTx (Fiber to the middle, wire, building or home) or another fixed line.

9.3.2 Quality

A quality indicator is the download rate of fixed broadband. Akamai publishes comparative statistics quarterly. Table 3 presents the comparison between Brazil and the same countries.

Table 3 Comparison of fixed broadband download rates in Brazil and selected countries, 3rd quarter of 2015[a].

Country	Average "*download*" rate (Mbps)	% Greater than 4 Mbps	% Greater than 10 Mbps	% Greater than 15 Mbps
Global Average	5.1	65	27	15
Brazil	3.6	32	2.2	0,6
Russia	10.2	87	38	15
India	2.5	14	2.3	0.8
China	3.7	33	1.6	0.3
South Africa	3.7	22	2,9	1.7
Argentina	4.2	39	3,1	0.5
Mexico	5.5	64	6.4	1.7
Uruguay	5.9	68	7.7	1.6
South Korea	20.5	96	68	45

Source: Akamai (2015)

Note: [a] Average speed of IP addresses connecting to Akamai servers, excluding wireless networks and cloud hosting services that typically have extremely fast connections to the Internet.

In addition to the download rate, it is important to consider other elements of broadband quality. There are no international statistics on the quality of access. In Brazil, due to continuing complaints about the poor quality of telecommunications services, in 2011 and 2012, Anatel set 14 targets for operators, including the Data Connections Drop Rate (<5%), the Contracted Instantaneous Transmission Rate Guarantee (> 95%) and the Contracted Average Transmission Rate Guarantee[126] (>80%)[127].

126 Defined as the simple arithmetic mean of the results of measurements of instantaneous speeds, carried out during a month. See <http://www.anatel.gov.br/legislacao/resolucoes/26-2011/57-resolucao-574>.

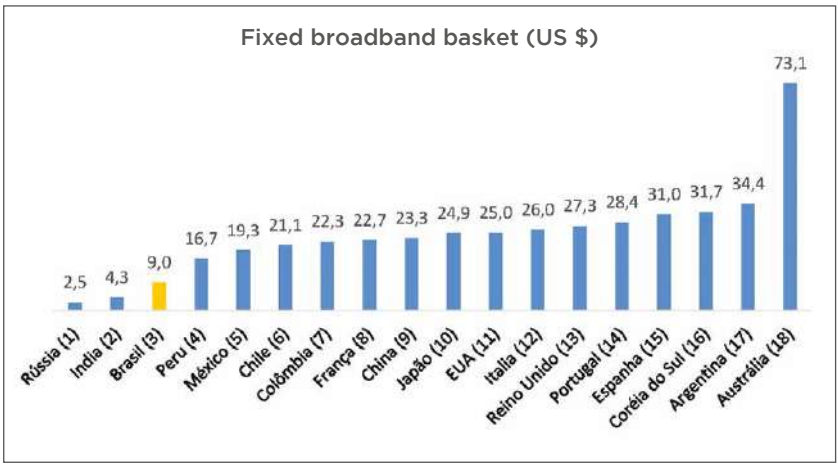
127 See <http://www.anatel.gov.br/dados/index.php?option=com_content&view=article&id=294&Itemid=539>.

For fixed broadband, considering the indicators of all the providers monitored in the first half of 2015, the percentage of compliance with service goals reached only 59.5%. This level was below that observed during the years 2012 (70.94%), 2013 (70.55%) and 2014 (67.85%)[128]. For mobile telephony, in the first half of 2015, the percentage of compliance with service goals reached 68.1%. This level was in line with what was verified in the years 2012 (66.97%), 2013 (68.75%) and 2014 (68.78%)[129].

9.3.3 Prices

The consulting company Teleco conducted a survey in November 2017 to compare fixed broadband prices in 18 countries. The Brazilian price was US $ 9.0, the third lowest of the 18 countries. (Teleco 2017)

Figure 1 Fixed Broadband Value in US $, November 2017.



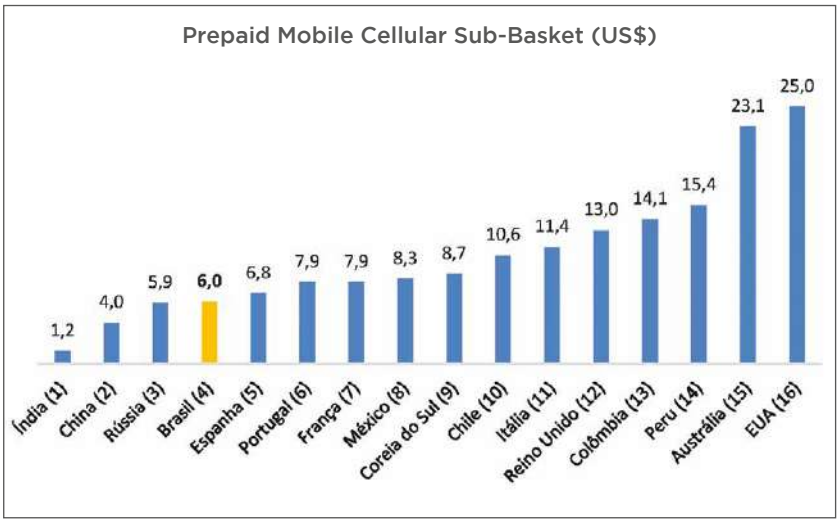
Source: Teleco (2017).

Teleco (2017) also conducted a comparative price survey of prepaid mobile broadband in November 2017, analyzing 18 countries, including Brazil. In this study, Brazil had prices lower than 14 of the 18 countries included in the research (Figure 2).

128 See <http://www.anatel.gov.br/dados/index.php?option=com_content&view=article&layout=edit&d=295>.

129 See <http://www.anatel.gov.br/dados/index.php?option=com_content&view=articlelayout=edit&id=296>.

Figure 2 Value of Mobile Prepaid Mobile Broadband for mobile phones in US $, November 2017.



Source: Teleco (2017).

9.4 Factors that affect the price of Broadband

Several factors affect the price of broadband. The most obvious is the high taxation (taxes, fees and "contributions") that affects telecommunications. Other factors that affect the price of broadband are the lack of competition in some markets, financing and installation costs of networks in remote areas and / or low level of disposable income and the high cost of space rental in power poles, electrical towers and / or fiber optic cables of other operators.

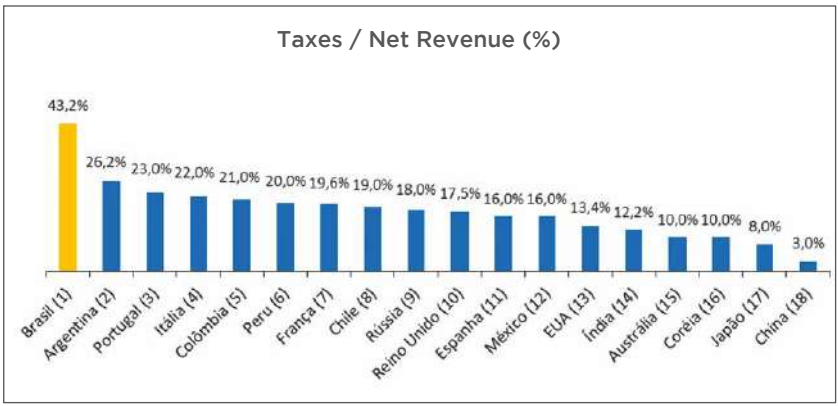
9.4.1 Taxes on telecommunications

In Brazil, the tax burden of this sector is among the largest in the world, 43% in 2015 (Figure 1.7) and in 2005 it was already the biggest among the eight economic sectors studied by Rogério Werneck, reaching more than double of the manufacturing sector (Werneck, 2008, Table 5). A detailed study by Teleco for Telebrasil in 2015 examined the taxation of the sector in Brazil and 17 other countries (Levy, 2015) indicating that Brazil had the highest

average tax burden (43%) among the countries in the sample, above Argentina, which comes in second place (26%).

Brazil's tax burden was more than double the average of the other 17 countries (16%). The study verified that the tax burden of Brazil was 65% higher than that of Argentina, the second highest among the countries analyzed, 139% more than that of Russia and 4.3 times more than that of South Korea (Figure 3). In 2016 the rate of the Tax on Circulation of Goods and Services (ICMS), the heaviest tax, rose an average of 3.9 percentage points in 11 states and in the Federal District, raising the national average tax burden (weighted by the number of cellular phones in each state) from 43 to 46%, and up to a maximum of 68.5% in the state of Rondônia. And this taxation does not include that of three sectoral funds mentioned in the next paragraph.

Figure 3 International comparison of taxes in the telecommunications sector, 2015.



Source: Levy, 2015.

The exceptionally high tax burden of this sector is not only a distortion that reduces the efficiency of investments, but also goes against digital inclusion policies promoted by federal, state and municipal governments. On top of that, the Ministry of Science, Technology, Innovation and Communications (MCTIC) has evidence that a reduction in current rates would increase government revenues, due to the increase in the demand for services more than proportional to the reduction in prices (Knight, 2014, p. 88-89

and Chapter 8 of Knight, Feferman and Foditch, 2016). From 2001 to 2015, BRL R$ 90 billion were raised in current prices (not adjusted for inflation) for three federal funds that must be used to support the telecommunications sector – the Telecommunications Services Universalization Fund (Fust), the Telecommunications Control Fund (Fistel) and the Technological Development Fund of Telecommunications (Funttel). But of that total, only 7% were applied to the stated objectives of these three funds[130].

9.4.2 Other factors that affect the price of broadband

The lack of competition between telecommunications companies in some markets can be a factor that influences the price of fixed broadband, since many regions and municipalities have only one or few suppliers, at least wholesale. However, competition is much greater for mobile broadband. There are four major mobile phone companies in Brazil: Vivo (Telefónica), TIM, Claro and Oi, which compete with each other, as well as with regional or smaller providers, like Algar and Nextel. Of the 5,665 Brazilian municipalities, in September 2015, 42% where 83% of the population live had between four and six operators competing in the personal mobile service – SMP (Telebrasil, 2015, Tables 4.11, p.105 and 4.14, p 109)[131].

The high costs of financing and implementation of networks are influenced by the high interest charged in Brazil, among the world's largest in real terms, the high taxes that affect these expenses and the difficulties in reaching remote regions in a huge territory.

The high cost of leasing infrastructure from other operators (for example, fibers or capacity in fiber optic cables, use of poles from state power distributors to hang fiber optic cables, cable ducts, spaces in antenna towers) is cited often as a problem by small and medium operators.

Finally, we can highlight the little investment of the public sector in cooperation. In the Pluriannual Plan (PPA) of the federal

130 For details of the sectoral funds, see Chapter 8, in Knight, Feferman and Foditch (2016).

131 For more details on the competition see Figures 4.9 and 4.10, Table 7.1 and Chapter 11 of this book.

government for the years 2012-2015, the investment in the National Broadband Program (PNBL) was projected at BRL 2.8 billion in the period 2012-2013. The budget laws for those years programmed only BRL 314.7 million. With the contingency of resources by the Ministry of Finance, the value was reduced to BRL 267.9. But budget execution was just BRL 214.1 million, just 7.6% of the PPA forecast (Diniz, 2014, p 17).

9.5 Federal broadband public policies in Brazil

Since 1989, before the arrival of the Internet in Brazil, the federal government has been promoting the growth of broadband, initially via the National Education and Research Network (RNP), since 1998 via privatization of the telecommunications sector and through the promotion of competition, and from 2002 on a variety of digital inclusion programs.

9.5.1 National Research Network Programs[132]

Since its creation in 1989, the RNP, today a social organization associated with the Ministry of Science, Technology, Innovation and Communication (MCTIC), promotes the expansion of broadband in Brazil. Starting in 1992, RNP offers broadband connection to research and higher education entities through a network of links initially provided by Embratel and, after the privatization of telecommunications in 1998, by several operators.

Beginning in 2007, starting in Belém do Pará, the RNP has been building its own metropolitan fiber optic networks in several cities, in partnership with teaching and research entities, state and municipal governments and several entities of the public and private sectors. The vehicle for this is the Redecomep Program, with financing from the federal government. In 2011, RNP inaugurated the sixth generation of its national backbone, the Ipê Network, with most of it being the result of an agreement of ten years, mediated by Anatel, with the operator Oi, which gave RNP the use of more than 20,000 km of its national fiber optic infrastructure.

132 For more details on the creation and expansion of the RNP, see Chapter 8 of Knight, Feferman and Foditch (2016).

As of 2012, RNP began to implement the Veredas Novas ("New Paths") program, with the objective of providing 1 Gbps and 100 Mbps connections to federal education and research institutions (and RNP clients) in locations outside the large urban centers, in the hinterland of the states. A part of these connections is provided by national and regional telecommunications operators, but the program also has a collaboration between RNP, Telebras and IT companies of the state governments, initially in Ceará (Etice) and Pará (Prodepa), to meet this demand for better connectivity for these academic clients.

At the end of 2017, the Ipê Network (the backbone of the RNP) included 27 Points of Presence (PoPs), one in each unit of the federation, as well as branches to serve around 1,500 units of research, health and higher education institutions throughout the country, benefiting more than 3.5 million users. Its length was about 22,000 km. The metropolitan networks program (Redecomep) currently has 26 networks in operation, in its first phase in operation, and a new network under construction, totaling 1,650 km. The second phase includes another 11 networks in operation and nine under construction, in a total of 600 km. Therefore, the total installed capacity reaches about 2,400 km of optical wiring. The new program of RNP, Veredas Novas, has already activated some 600 circuits of 100 Mbps and 1 Gbps, with an average of 200 km each from the point of presence in the state of the RNP, totaling about 120,000 km.

9.5.2 Privatization of telecommunications and promotion of competition

The privatization of telecommunications in Brazil dates back to 1998, based on the General Telecommunications Law – Law 9742 (LGT) of 1997, which also created the National Telecommunications Agency (Anatel), which regulates telecommunications and promotes competition in the telecommunications sector. The end of state monopolies and the promotion of competition among large, medium and small private companies were of fundamental importance both for the expansion of broadband infrastructure and for the reduction of prices for telecommunications services (although the cost of broadband remains high).

Competition was also favored by the existence of a large number of small and medium-sized local and regional providers of Internet and telecommunications services. This large participation of small and medium suppliers is a marked characteristic of the Brazilian market. There about 8,000 suppliers, of which there are 4,000 formalized with Anatel licenses[133].

9.5.3 National Broadband Program[134]

Created by Decree n 7.175/2010, the PNBL is an initiative of the federal government whose main objective is to spread broadband Internet access in the country, mainly in the most inaccessible regions.

The goal of the PNBL was to have 35 million households connected to the global computer network in 2014. The MCTIC worked on several fronts, the most important being the tax reduction of access networks and terminals, the Special Regime for Taxation of the National Broadband Program (REPNBL), the Popular Broadband program and the expansion of the public fiber optic network. (managed by Telebras, a federal state company reactivated in 2010).

Up to 2014, 32.3 million households had an Internet connection, of which 21.7 million were fixed broadband (62% of the PNBL target) and 6.7 million fixed broadband with a transmission rate greater than 4 Mbps (CETIC, 2015, Tables A4-A6, pages 322-324). In 2014, the Popular Long Band package was offered wholesale in 4,157 municipalities and retail in 5,376 municipalities, 90% of the 5,565 Brazilian municipalities (Telebrasil, 2015, Table 2.20, page 58). However, the number of accesses in the popular package was only 2.6 million in June 2014 (MCTIC, 2014). This suggests that the vast majority of the BLP contracts were in the state of São Paulo.

One of the main objectives of the PNBL was to build a national broadband network, that is,

> a set of infrastructure and operation that supports the formulation of public policies related to the massification of access not only to the internet, but also to government content that induces social inclusion, the

133 See Chapter 10 of Knight, Feferman and Foditsch (2016) for an analysis of the role of small and medium-sized Internet and telecommunications providers.

134 See Chapter 2 of Knight, Feferman and Foditsch (2016) for more details on the PNBL.

> exercise of citizenship, promotes education and digital culture, among others [...] (CPID, 2010, pp. 41-42)

The responsibility to reach that goal was delegated to Telebras, which was to reach 4,278 municipalities with its fiber optic network in 2014. However, the state company reported that it only reached 612 municipalities, 360 through direct offer and 252 through partners (Diniz, 2014, p.17).

Senator Anibal Diniz, rapporteur of an evaluation of the PNBL for the Federal Senate (Diniz, 2014), wrote in his report that the budget execution of Telebras related to the PNBL in its first four years was around R$ 284 million, 7,4% of the planned budget. In addition, the Digital Inclusion Program Management Committee had not met since 2010 and had not submitted the PNBL monitoring reports that were its responsibility. The Connected Brazil Forum, created to bring together more than 60 institutions from governments, civil society and the private sector, was deactivated (Reis & Fontenelle, 2014 e Diniz, 2014, pages 17 and 32).

It should be noted that the information available from Telebras on its site is very scarce and not very transparent. The last available analysis of the MCTIC, presented in June 2014, shows data of Telebras coverage in 2013 and plans for implementation in 2014. The vast majority of the Telebras network consists of fibers in the leased OPGW cables of the companies of the state group Eletrobras. Telebras indicates on its site that at the beginning of March 2016 its fiber optic network was 28,000 km[135].

9.6 Conclusions

In these conclusions, we highlight three topics: (1) the importance of the use of integral strategic planning of ICTs and its analogical complements to accelerate the economic, social and political development of the country; (2) the evolution of broadband in Brazil compared to other countries and (3) federal government programs for the expansion of broadband and digital inclusion.

135 See <http://www.telebras.com.br/inst/?page_id=8>.

9.6.1 Lack of strategic planning

There is no national strategy for the use of ICTs to accelerate the social, economic and political development of Brazil. The only attempt was the Green Paper (Takahashi, 2000) published by the MCTIC (then MCT). It has never been implemented. The PNBL, launched in 2010, does not include a holistic strategy to take advantage of ICT. It is limited to the expansion of broadband.

9.6.2 Broadband in Brazil and other places

Despite significant improvements, the Internet reached only 54% of households in 2016, only 12% with 8Mbps or more. All these indicators are worse for rural areas, less developed regions, the poor, the less educated and the old. The penetration of broadband, transmission rates and broadband prices in Brazil leave much to be desired. Compared with countries with levels of development similar to Brazil, with some exceptions, Brazil does not score well in these indicators.

9.6.3 Federal programs for expanding broadband and digital inclusion

The expansion of broadband in Brazil has not been a priority of the governments of Fernando Henrique, Lula or Dilma. In the two governments of Fernando Henrique, the priorities were the privatization of telecommunications companies, the establishment of Anatel to regulate these companies and electronic government. In the governments of Lula and Dilma, e-government was left aside and the emphasis was given to digital inclusion, largely due to the obligations imposed on private companies and then to the expansion of broadband since the launch of the PNBL in 2010; it only achieved 62% of its main goal. Despite President Dilma's declarations as of 2014, the promised BLPT was not launched.

Union budgets dedicated to digital inclusion and broadband expansion have been extremely small, and on top of that these resources have been misused by the Ministry of Finance (as in the case of Telebras).

The Ministry of Finance also appropriated almost all the financial resources of FUST and most of FISTEL and FUNTTEL and

dedicated it to uses that have nothing to do with the development of telecommunications. These resources could have been used to promote inclusion and digital literacy, make public investments and / or encourage private investment. The tax burden of the sector is one of the largest in the world, with a negative impact on prices and on the capacity of the private sector to invest in the expansion of networks. The decreases of the REPNBL (called tax expenditures by economists) have been very small compared to the enormous tax burden imposed on the telecommunications sector.

Recent legislative initiatives were not approved by Congress until February 2018. They include the bill for a new Telecommunications Law (PLC 79/2016) that aims to prioritize investments in broadband, and to replace fixed telephony as well as two other bills that seek to liberate FUST so that its resources are applied in services provided by private companies (PLS 4277 and PLS 125, both of 2017). The approval by Congress and sanction by the President of Brazil of these bills would be a great step forward to stimulate investments in broadband infrastructure.

The reduction of the tax burden that increases the cost of broadband would be a very effective measure to stimulate the expansion of broadband infrastructure in the country, but initiatives in this regard continue to be challenged by the federal and state tax authorities.

Government programs to promote digital literacy to complement the expansion of infrastructure would be useful and probably much cheaper than direct investments in broadband infrastructure. This is all wrong. Substitute:

> These could be financed through direct federal funds (e.g., courses in federal universities), state funds (e.g., courses in state universities and secondary schools), and municipal funds (e.g., primary school courses); or via incentives and/or subsidies for private entities, be it formal teaching institutions or others (e.g., Lan Houses, a Brazilian equivalent to “Internet cafés”).

9.7 References

Akamai (2015). Akamai's State of the Internet 3rd Quarter 2015. Vol.8 No. 3. <https://www.stateoftheinternet.com/downloads/pdfs/2015-q3-state-of-the-internet-report.pdf>.

Anatel, Secretaria Executiva (2011). Proposta de Plano Geral de Metas de Competição – PGMC. Apresentação na Audiência Pública, Consulta Pública No 41, 26 de julho de 2011. <http://www.anatel.gov.br/Portal/ documentos/sala imprensa/5-9-2011--14h19min56s-PGMC%20-%20Apresenta%C3%A7%C3%A3o%20Audiencia%20Publica.pdf>.

Borges, A. (2015, 10 dezembro). Fundos de Telecom bancam até ferrovia. O Estado de São Paulo. <http://economia.estadao.com.br/noticias/geral, fundos-de-telecom-bancam-ate-ferrovia,10000004524>.

Bruno, L. (2014, 30 setembro). Programa de banda larga se aproxima do fim criticado por entidades e operadoras. Reuters. <http://br.reuters.com/article/domesticNews/idBRKCN0HP2CO20140930>.

Comitê Gestor da Internet no Brasil (CGI.br). TIC Domicílios e Empresas: Pesquisa sobre o uso das tecnologias de informação no Brasil, volumes para os anos 2005-2014. São Paulo: NIC.br e CETIC.br, 2007-2017. <http://cetic.br/publicacoes/indice/pesquisas/>.

Comitê Gestor do Programa de Inclusão Digital – CGPID, Secretaria Executiva (2010). Plano Nacional de Banda Larga. <http://www.mc.gov.br/component/docman/cat_view/22-acoes/30-programa-nacional-de-banda-larga-pnbl?Itemid=13217>.

Diniz, A. (2014). Avaliação do Programa Nacional de Banda Larga (PNBL). Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática (CCT) do Senado Federal, 2 de dezembro de 2014. <http://www.senado.gov.br/atividade/materia/getPDF.asp?t=157729&tp=1>.

Dutta, S.; Geiger, T.; Lavin, B. (2015). The Global Information Society Report 2015: ICTs for Inclusive Growth. Genebra: World Economic Forum.

Ferreira, M. (2015). A arrecadação e a destinação dos fundos das Telecomunicações. Apresentação para Audiência Pública – 17 de junho de 2015. Brasília: Ministério das Comunicações. <http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cctci/audiencias-publicas/2015/17-06-2015-ap-fundos-das-telecomunicacoes/marcelo- leandro-ferreira-minicom>.

Instituto Brasileiro de Geografia e Estatística (IBGE) (2015). Pesquisa Nacional por Amostra de Domicílios 2014. Tabelas disponíveis em: <http://www.sidra.ibge.gov.br/pnad/default.asp>.

Knight, P. (2014) A Internet no Brasil: Origens, Estratégia, Desenvolvimento e Governança. Bloomington, Indiana: AuthorHouse.

Knight, P.; Feferman, F.; Foditch, N. (2016). Banda Larga no Brasil: Passado, presente e futuro. São Paulo: Novo Século. <https://www.dropbox.com/home/Broadband%20in%20Brazil>.

Levy, E. (2015). Telecomunicações no Brasil. Apresentação na Audiência Pública na Comissão de Fiscalização Financeira e Controle da Câmara dos Deputados. 17 de setembro de 2015. <http://www.telebrasil.org.br/posicionamento-apresentacao/7985-tributacao-no-setor-de-telecomunicacoes-17-09-2015.

Ministério das Comunicações (2014). Programa Nacional de Banda Larga – PNBL: Situação em junho de 2014. Apresentação. <http://www.mc.gov.br/component/search/?searchword=PNBL&ordering=newest&searchphrase=all>.

Ministério da Fazenda (2015). Análise da Arrecadação das Receitas Federais, Dezembro /2014. Brasília: Secretaria da Receita Federal, Centro de Estudos Tributários e Aduaneiros, 20 de janeiro de 2015. <http://idg.receita.fazenda.gov.br/dados/receitadata/arrecadacao/relatorios-do-resultado-da-arrecadacao/2014/dezembro2014/analise-mensal-dez-2014.pdf>.

Ministério da Fazenda (2015). Demonstrativo dos Gastos Tributários: PLOA 2015. Brasília: Secretaria da Receita Federal, Centro de Estudos Tributários e Aduaneiros, sem data. <http://idg.receita.fazenda.gov.br/dados/receitadata/renuncia-fiscal/previsoes-ploa/arquivos-e-imagens/dgt-2015>.

Reis, A. & Fontenelle, A. (2014, 2 dezembro). Banda larga maior depende de recursos e gestão articulada. Jornal do Senado. Disponible en: <http://www12.senado.gov.br/jornal/edicoes/2014/12/02/banda-larga-maior-depende-de-recursos-e-gestao-articulada>.

Sardemberg, C. A. (2013, 21 marzo). Nos balcões do governo. O Globo. <http://oglobo.globo.com/opiniao/nos-balcoes-do-governo-7898784>.

SindiTelebrasil (2015). Setor de Telecomunicações em 2015. Apresentação, Brasília, 24 de novembro de 2015. <http://www.telebrasil.org.br/posicionamentos/posicionamentos/apresentacoes?start=4>.

Takahashi, T. (2000). Sociedade da Informação no Brasil: Livro Verde. Brasília: Ministério da Ciência e Tecnologia. <http://livroaberto.ibict.br/bitstream/1/434/1/Livro%20Verde.pdf>.

TELEBRASIL (2015). O Desempenho do Setor de Telecomunicações no Brasil: Séries Temporais 9M15. Rio de Janeiro, dezembro de 2015. <http://www.telebrasil.org.br/panorama-do-setor/desempenho-do-setor>.

Teleco (2017). Preços no Mundo: Benchmarking Internacional. 21 de novembro de 2017. <http://www.teleco.com.br/precos_pais.asp>.

Unión Internacional de Telecomunicaciones (UIT) (2014). Measuring the Information Society Report 2014. <http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf>.

Unión Internacional de Telecomunicaciones (UIT) (2016). Measuring the Information Society Report 2016. <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-w4.pdf>.

Werneck, R. (2008). Tax reform in Brazil: an evaluation at the crossroads. Texto para Discussão n. 558, Departamento de Economia, PUC-Rio, janeiro de 2008. <http://www.econ.puc-rio.br/pdf/td558.pdf>.

10 Network Neutrality, Zero-Rating and the *Marco Civil da Internet*

Luca Belli

Note: *This chapter is an updated version of the article published, with the same title, in Del Campo A. (Ed.) (2017). Towards an Internet free of censorship II. Perspectives in Latin America.*

Abstract

This chapter explores the evolution of the debate on net neutrality starting from an international perspective, and then focusing on the Brazilian case, where the practice of sponsoring specific applications, the so-called zero rating, is analysed. Discussions on these issues have intensified considerably in recent years, covering the whole of Latin America, and more specifically Brazil, where Law 12,965, known as the *Marco Civil da Internet*, and its regulation, decree 8,771 of 2016, have regulated the protection of several fundamental rights in the online environment and have guaranteed the protection of net neutrality in Brazil. Internet traffic discrimination practices, the diffusion of so-called zero rating models and, consequently, discussions about the principle of non-discrimination, called net neutrality, have taken on considerable proportions in the region. This popularization of the debate on net neutrality is due to the increasing awareness that a non-discriminatory access to the Internet is essential to preserve the full enjoyment of the fundamental right to communicate, and the possibility to share innovation and do business freely online. After a discussion on net neutrality, this chapter offers a critical analysis of zero rating practices exploring how they are regulated in the *Marco Civil da Internet*. Finally, it explores the potential negative effects of these practices and points to future ways to address Internet access issues in a sustainable manner.

10.1 Introduction

During the last decade, nework neutrality (NN) has been a subject deeply analyzed throughout the world, involving multiple actors both in Brazil and in various international forums. NN is defined as

the principle of non-discrimination whose purpose is to preserve the openness of the Internet and to facilitate the end user's full enjoyment of their rights. For these reasons, NN has been enshrined in various national and international regulatory instruments. In Brazil, NN is explicitly protected by Law 12.965 (2014), better known as the Civil Rights Framework for the Use of the Internet in Brazil, or *Marco Civil da Internet* (MCI), which is the federal law that establishes the fundamental principles and rules that govern the use of the Internet in Brazil.

The evolution of the debate on NN strongly influenced the consultations and Congress debates leading to the elaboration of the MCI and the presidential decree that specifies some provisions of the MCI. Particularly, it should be noted that the public consultations that led to the development of the decree revealed that *Zero Rating* (ZR) and its compatibility with NN was one of the most debated and complex issues in the consultations. ZR is the practice of sponsoring access to certain applications that do not affect the user's monthly data capacity. The analysis of these practices has been strongly present in almost all the debates about net neutrality in recent years. The purpose of this article is to contextualize NN and ZR in order to explain the recent development of policies and regulations in Brazil and to draw lessons that may be useful in other contexts.

The first section of this chapter examines the foundations of NN, provides an overview of the debates held on the subject, and highlights the fundamental role of the principle of neutrality in allowing the full enjoyment of the fundamental rights of Internet users. Consequently, the analysis of the second section revolves around the MCI and its key function as a promoter of human rights and, particularly, the full exercise of citizenship, universal access and innovation, highlighting that the MCI considers NN as one of the fundamental principles allowing the achievement of these objectives, while guiding the discipline and the use of the Internet in Brazil.

The case of Brazil provides an interesting example of, the formal inclusion of NN together with constitutional values, such as the protection of human rights and the promotion of innovation. On the other hand, the Brazilian case also tellingly illustrates that most

widespread ZR offers[136] tend to greatly reduce the openness of the Internet, as they steer and *de facto* restrict the use of the Internet to a limited number of subsidized applications[137]. In this regard, the combination of limited data allowance and sponsored services – whose data consumption is not limited – could considerably limit the possibility of freely choosing how to utilize one's Internet connection, especially for users with more limited financing capacity, transforming the Internet into a network of predefined purpose. It should be remembered that the Internet is a general purpose network, where each user freely chooses what he wants to do with his connection, accessing and freely sharing content and applications that the user can freely create. On the contrary, the combination of very limited data caps and a restricted selection of sponsored services can transform the Internet into a network of predefined purpose, as it directs usage towards the sponsored services rather than the most interesting or those having the best quality, thus creating a toll for the free – meaning without restriction – use of the Internet and directing users towards the use of dominant sponsored services.

In fact, for ZR practices to be interesting for – especially underprivileged – consumers the combination of these practices with limited data allowance is essential because sponsoring access to certain applications becomes interesting for consumers only when their data allowance is limited and, therefore, they have an advantage in receiving sponsored access to specific services. On the contrary, when the monthly volumes of data are not limited or when such limits are very wide, the user does not need sponsored services because all services are accessible without fear of consuming data. Thus, in the absence of data limits, the only criterion for choosing applications is quality and interest of a specific service, and not the fear of consuming valuable data. In this context, the possibility of implementing any ZR model may represent an incentive for operators to keep the monthly data limit as low as possible to be able to direct the attention of their users towards the services of its business partners, instead of promoting

136 For an overview of the most widespread ZR plans in the world, see <http://www.zerorating.info/>.

137 For more information on which applications are included in the ZR plans in Brazil and in other countries, see <http://www.zerorating.info/>.

the use of an open Internet. Indeed, directing users' attention becomes incredibly valuable considering that attention and use of a specific app means collection of personal data of the users, which is the most valuable resource of the "*attention economy*"[138].

In this scenario, Internet users can be transformed *de facto* in mere consumers of pre-selected applications, using their connection only as passive users of predefined services. ZR practices, therefore, have the potential to turn users into simple data producers instead of preserving their peculiar characteristic of "prosumers", that is, being consumers and producers of innovation and information. The most recent data from the Brazilian Institute of Geography and Statistics corroborate this scenario, highlighting that 94.5% of Brazilian mobile users utilize the Internet mainly for instant messaging applications[139]. Considering that most Brazilian mobile users have prepaid plans[140] which include limited data volumes and *zero rated* messaging applications (typically the WhatsApp), it is natural to wonder if Internet users use the Internet mainly for sending and receiving messages because this is what they want or because it is the only free option that, therefore, is becoming an induced habit.

In this context, we must also reflect on how ZR models can impact the functioning of democracy and the independent formation of the opinions of citizens. In Brazil, lower-income users are those who mainly use prepaid plans[141] which include ZR. These users receive and disseminate (mis)information essentially participating in groups on WhatsApp and via Facebook that are among the few sponsored applications in the country[142].

---

138 See Belli L. (2017). The scramble for data and the need for network self-determination. OpenDemocracy <https://www.opendemocracy.net/luca-belli/scramble-for-data-and-need-for- network-self-determination.

139 See Agencia IBGE. (February 21, 2018). PNAD ContinuousICTs2016: 94.2% of people who would use the Internet or fizeram to exchange messages. <https://tinyurl.com/y95fy8qn>.

140 According toICTsdomiciliary research, in 2016, 73% of Brazilian mobile users used prepaid plans. See Cetic.br. (2016: 388) TIC DOMICILLIOS: Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação nos Domicílios Brasileiros <http://cetic.br/media/docs/publicacoes/2/TIC_DOM_2016_LivroEletronico.pdf>.

141 According toICTshome research, 79% of lower renda – D and D classes – use prepaid plans. See *Idem.*

142 See Belli L. (December 5, 2017). Neutralidade de rede e ordem econômica. Observatory of Marco Civil gives Internet. <http://www.omci.org.br/jurisprudencia/207/neutralidade-de-rede-e-ordem-economic/>.

Several studies have already shown that disinformation is disseminated more rapidly and pervasively and encourages a much higher articipation than the real news articles among Brazilian netizens[143]. Most of these users use prepaid plans with *zero rating* and become particularly vulnerable to the spread of so-called "fake news" because it is very difficult for them to verify if the information received is true or if it is fabricated, since access to informative material and sources of independent analyses, which would allow verification, is not sponsored but, to be accessed, has to be paid for by users.

After analyzing the ZR phenomenon in Brazil and its compatibility with the MCI, this article will propose some final considerations and some suggestions about the policies that could promote digital inclusion, without the need to use ZR schemes, namely: the promotion of "community networks" that can greatly expand access to the Internet, empowering individuals and generating positive progress among previously disconnected communities, while avoiding to generate the negative externalities produced by ZR.

10.2 The net neutrality debate

The proliferation of debates on NN has stimulated the generation of national and international policies to promote and protect this non-discrimination principle[144]. Although several nuances of NN have been proposed, most of the actors agree on the essence of it and define it as "the principle according to which all Internet traffic must receive the same treatment, without discrimination, restriction or interference, regardless of its sender, receiver, type, content, device, service or application"[145]. However, there is a great debate about the concrete implementation of this principle, and NN discussions have frequently generated controversies regarding what should be considered a "reasonable" management of Internet traffic and the need (or not) to regulate traffic management.

143 See, for example, Alexandre Aragão Craig Silverman (22 Novembro 2016) The Top Fake News Stories Outperformed Real News About A Major Scandal In Brazil, Too. <https://tinyurl.com/y7nv7j7p>.

144 See Belli and De Filippi (2016).

145 Internet Governance Forum (IGF), "Policy Statement on Network Neutrality", results of the XV United Nations Forum on Internet Governance, November, 2015, § 1.

Controversies about NN focus on the degree of freedom that network operators must have to implement Internet Traffic Management (ITM) techniques, which can "discriminate" content, applications and specific services that transit their electronic networks. Although it may seem a purely technical problem, the ITM carries enormous social, legal and economic implications. The implementation of a differentiated treatment may unduly limit the freedom of expression of users or competition, when such measures are not necessary and proportionate for the fulfillment of a legitimate objective[146].

Strictly speaking, the debate on net neutrality gained special relevance, since ITM's techniques can not only be used for a legitimate purpose, but also to harm the services of the competition, blocking or improperly degrading them, or to favor business partners through prioritization[147]. These undue limitations are possible in the absence of net neutrality policies, and have been demonstrated in a variety of national contexts, such as in the United States[148], Chile[149] or the EU[150], triggering the creation of frameworks for net neutrality.

It is important to mention that the ITM is not something negative *in toto* and that several types of ITMs play a fundamental role in ensuring the proper functioning of electronic networks, for example, by preserving the security and integrity of networks. However, operators may misuse the ITM techniques to favor

146 Belli, Luca and Van Bergen, M., "Protecting Human Rights through Network Neutrality: Furthering Internet Users', Interest, Modernizing Human Rights and Safeguarding the Open Internet," Council of Europe, CDMSI, Strasbourg, December 2013, Misc. 19, available in: <http://bit.ly/2fMPiKB>; Federal Communications Commission FCC. Report and Order on Remand, Declaratory Ruling, and Order on the Matter of Protecting and Promoting the Open Internet. GN Docket No. 14 28 2015; Belli and De Filippi, *supra* note 2; and Council of Europe (CoE), Recommendation CM / Rec (2016) 1 of the Committee of Ministers to the Member States on the Protection and Promotion of the Right to Freedom of Expression and the Right to Privacy Regarding the Neutrality of the Network, January, 2016, available in: <http://bit.ly/2f8FlWS>.

147 Body of European Regulators for Electronic Communications (BEREC), "A View of Traffic Management and other Practices Resulting in Restrictions to the Open Internet in Europe", in: *Findings from BEREC's and the European Commission's Joint Investigation*, BoR (12) 30, May 29, 2012; and FCC, *supra* note 4.

148 Federal Communications Commission (FCC), *Madison River Communications, LLC and affiliated companies*, Acct. No. FRN: 0004334082, Washington DC, 2005. Available in: <http://bit.ly/2f8Dul1>; Federal Communications Commission (FCC), "Commission Orders Comcast to End Discriminatory Network Management Practices", FCC News Media Information 202 / 418-0500, August 1, 2008. Available in: <http://bit.ly/2cpWlsb>.

149 Court of Defense of Free Competition (TDLC), "*Voissnet vs. CTC*", Judgment 45, October 2006.

150 BEREC, *supra* note 5.

or harm specific services, when the ITM is based on purely commercial considerations. In fact, the technological evolution of the last fifteen years has allowed operators to use ITM techniques that point or are directed to applications, services and specific contents, using measures known as "*application specific*". Such measures can be used in an abusive manner to discriminate, for example by blocking or degrading the quality of applications that compete with the applications offered to the trading partners of the operators[151]. In this sense, it is understandable that vertical integration[152] of network operators with Content and Application Providers (CAPs) offers concrete incentives for operators to privilege the traffic of business partners, by blocking or slowing down[153] of the services of the competition and the implementation of policies of paid priorization[154].

Therefore, while the ITM can offer benefits that improve the well-being of both users and operators, it can be used for abusive purposes that only benefit a very limited number of actors, that is, operators with market power and their commercial partners.

Such undue discrimination can have disastrous consequences not only for free competition, but also for the freedom of users to seek, impart and receive information without interference, a principle that is guaranteed by a series of international legal instruments and by most of the National Constitutions in force[155].

---

151 BEREC, *supra* note 5; Broadband Internet Technical Advisory Group (BITAG), "Port Blocking", to Broadband Internet Technical Advisory Group Technical Working Group Report, August 2013. Available in: <http://bit.ly/2fQYnVb>.

152 It should be mentioned that the phenomenon of vertical integration does not only concern network operators, since it is also related to online platforms (European Commission, Antitrust: Commission sends statement of objections to Google on comparison shopping service; on Android. 2015 <http://europa.eu/rapid/press-release_IP-15-4780_en.htm>. While this latter type of vertical integration can potentially harm the openness of the Internet and deserves the attention of regulators, it should be mentioned that NR policies are not concentrated in online platforms, but rather in operators that act at the level of access (BEREC, *supra* note 5; FCC, *supra* note 4; Belli and De Filippi, *supra* note 2).

153 This practice is also known as "filtering" and includes techniques that specifically limit the loading and unloading speeds of certain types of data flow. It has also been considered controversial when it is not disclosed transparently and is used to discriminate the flow of data from competing services.

154 Paid priorization refers to the practice of granting preferential treatment to the data flow of the trading partners of the operators. The operators present this practice as a technique to offer content with a guaranteed quality of service. Prioritization pays has been criticized for its potential to create "fast Internet routes" and "dirty routes", thus favoring business partners and harming those services that lack the financial capacity to pay for priority.

155 Belli and De Filippi, *supra* note 2.

However, it should be noted that NN is not an absolute principle and that there are exceptions in relation to reasonable traffic management. While it is true that discriminatory traffic management has its benefits when it is necessary and proportionate for the fulfillment of specific legitimate purposes[156], the problem is to what extent traffic management practices can be considered as legitimate, necessary and proportionate. In this regard, it should be mentioned that, although divergent views exist in relation to ITM, in general, the various *stakeholders* agree that discriminatory traffic management can be considered reasonable as long as it is necessary and proportionate for security and integrity of the network, or to prioritize emergency services, in case of force majeure, or when discrimination of specific protocols[157], instead of specific applications, becomes necessary in order to mitigate the effects of congestion[158].

In addition, the use of *Content Delivery Networks* (CDNs)[159] is generally considered compatible with NN, since such networks improve performance and decompress congestion by adding additional capacity to electronic networks, instead of degrading other communications that are transmitted by the same routers[160].

156 BEREC, *supra* note 5; FCC, *supra* note 4; IGF, *supra* note 3.

157 The term "specific protocol" describes a GTI technique that addresses a class of applications that run on a specific protocol, such as VoIP (voice over IP). Unlike the GTI of "specific applications", which addresses a specific application, the GTI of "specific protocols" points to a whole class of applications that exploit the same protocol. The term "specific protocol" differs from "independent protocol" (agnostic protocol), since the latter defines a GTI technique that does not address or affect any specific class of applications. *See*, Bastian et al. (2010). Comcast's Protocol-Agnostic Congestion Management System. RFC 6057. <https://tools.ietf.org/html/rfc6057>.

158 It should be noted that the analysis of the phenomenon of congestion is not as simple as it seems. In fact, it is particularly difficult to objectively identify the true cause of network congestion. As Frieden put it: "The true cause of congestion (...) remains elusive. Content creators and distributors speculate whether ISPs have deliberately caused congestion, by refusing to optimize network capacity, or by allocating an available capacity that generates the probable traffic congestion of certain types and sources of content. ISPs deny this scenario and point to less perverse circumstances such as weather, vacations at home and the decision of content distributors, such as Netflix, to broadcast episodes for the entire season. "*See* Frieden, Rob, "Net Bias and the Treatment of 'Mission-Critical' Bits," Paper TPRC Conference, March 24, 2014. Available in: <http://bit.ly/2eXhbRE>.

159 CDNs are network systems that act as intermediaries between the source of an application provider and the operator, with the aim of accelerating the transmission of data. See Pallis, George and Vakali, Athena, "Insight and Perspectives for Content Delivery Networks", Communications of the ACM, Vol 49, No. 1, January 2006, available at: <http://bit.ly/2fNh5us>. This is achieved with the *hosting* local of the selected data copies *(mirroring)*, and at the request of the end user, the CDN intercepts the request and sends the data from the local hosting point instead of sending it from the remote source. Thus, CDNs improve performance by shortening the total distance that the data packets must travel until they reach their destination.

160 BEREC, *supra* note 5; FCC, *supra* note 4.

In addition to being used to manage the phenomenon of congestion, the actions of ITM can also be useful in dealing with malicious use of the Internet, such as *spam*, cyber-attacks and content and services considered illegal.

However, as mentioned above, although several network operators acquired the capabilities to handle Internet traffic more accurately and efficiently, for example, filtering the spam or prioritizing applications sensitive to latency in case of congestion, they also acquired concrete incentives to discriminate specific resources for expressly commercial reasons. In this context, ITM techniques can be used to ensure the proper functioning of the Internet, but also to favor or harm specific services and contents, by having the ability to distort the market and alter the freedom of users to search, impart and receive information without interference. In this sense, several Internet companies have expressed that network operators "are motivated to discriminate and block Internet traffic, have the tools to carry it out and the ability to hide their actions, blaming other actors"[161].

10.2.1 An Internet Traffic Management Compatible with Human Rights

It is important to highlight that dicriminatory ITM can be used for anticompetitive behaviours but can also lead to the violations of fundamental rights of internet users and, particulerly, their freedom of expression. The traditional conception of freedom of expression consist in the state's negative obligation of non interference with people's ability to freely seek, impart and receive information and ideas. At at the same time, freedom of expression includes the state's positive obligation to protect individuals from the adverse effects that may experience due to the activities of other individuals and companies[162]. In this regard, the jurisprudence of the Inter-American

161 Internet Association, Comments of the Internet Association in response to the Federal Communications Commission's ("Commission" or "FCC") May 15, 2014 Notice of Proposed Rulemaking ("NPRM" or "Notice"), GN Docket No. 14-28. <http://internetassociation.org/wp-conten/uploads/2014/07/Comments.pdf>.

162 *See* Human Rights Committee in its General Comment No. 31. March 29, 2004. <http://www.unhcr.org/4963237716.pdf>; Commissioner for Human Rights of the Council of Europe (UNHCR), reports on the rule of law and the Internet, December 2014, § 8; European Court of Human Rights, "*L fish Ostra v. Spain* ", Judgment No. 16798/90, §44-58, December 9, 1994; European Court of Human Rights, "*Khurshid Mustafa and Tarzibachi v. Sweden* ", Judgment No. 23883/06, December 16, 2008.

Court of Human Rights (Inter-American Court of Human Rights) and the European Court of Human Rights (ECHR) is very clear in relation to the importance of the non-discriminatory treatment of information and ideas. The Inter-American Court consistently establishes that "equality must regulate the flow of information," and emphasizes that the State has a positive obligation to "extend the rules of equality to the greatest possible extent, to allow the participation of different information in the public debate, promoting informational pluralism"[163]. On the other hand, the ECHR has continuously expressed that freedom of expression "applies not only to the content of information, but also to the means of dissemination, since any imposed restriction will necessarily interfere with the right to receive and impart information"[164].

These considerations have also been continually reiterated by the special rapporteurs for freedom of expression, who took a proactive approach towards the protection of NN, emphasizing that "the processing of data and Internet traffic should not be subject to any type of discrimination based on factors such as devices, content, author, origin and / or destination of the material, service or application[165].

Therefore, European governments have decided to explicitly protect NN as a human rights norm. In fact, the 47 members of the Council of Europe have reflected the protection of NN in a Recommendation of the Committee of Ministers[166], reiterating its commitment to the net neutrality principle, already openly expressed in the Declaration on Network Neutrality of 2010[167].

These commitments arise from the observation that non-discriminatory access and circulation of content, applications and

163 IHR Court, *"Kimel vs. Argentina"*, judgment of May 2, 2008, Merits, reparations and costs, Series C, No. 177, § 57; IHR Court, *"Fontevecchia and D'Amico vs. Argentina"*, judgment of November 29, 2011, Merits, reparations and costs, Series C No. 238, § 45.

164 European Court of Human Rights, (ECHR). "Autronic AG v. Switzerland ", 22 May 1990. Sentence No. 12726/87. <http://hudoc.echr.coe.int/eng?i=001-57630>; EHR (2012). "Ahmet Yıldırım v. Turkey. "Judgment No.: 3111/10. <http://hudoc.echr.coe.int/fre?i=001-115705>.

165 European Court of Human Rights, (ECHR). "Autronic AG v. Switzerland ", 22 May 1990. Sentence No. 12726/87. <http://hudoc.echr.coe.int/eng?i=001-57630>; EHR (2012). "Ahmet Yıldırım v. Turkey. "Judgment No.: 3111/10. <http://hudoc.echr.coe.int/fre?i=001-115705>.

166 Frank LaRue (UN), Dunja Mijatovic (OSCE), Catalina Botero Marino (OAS) and Faith Pansy Tlakula (CADHP), Joint Declaration on Freedom of Expression and Internet of the Special Rapporteur, June 2011. Available at: Available at: <http://bit.ly/1wnId8U>.

167 The author of this chapter had the honor of being the co-author of the report that originated the first draft of the recommendation. Compare Belli, Luca and Van Bergen (2013) and the Council of Europe Recommendation CM / Rec (2016) 1.

services not only facilitate the free exchange of information, but also contribute to reducing barriers to enter the market of creativity and innovation. In this sense, it is important to reiterate that Internet users are characterized as "prosumers", that is, they are not only consumers of information, but also producers of innovations that can compete with existing services and can potentially be disruptive. For this reason, a large number of *stakeholders* point out that NN is fundamental to "preserve the openness of the Internet, promoting the human rights of users and promoting competition and equal opportunities, safeguarding collaboration among peers and disseminating the benefits of the Internet to all people"[168].

Strictly speaking, in the digital environment, the freedom to receive and transmit ideas means freedom of access and diffusion of innovation, which contributes actively to the evolution of the Internet. Thus, by reducing the possibility for operators to interfere with user freedom of expression, non-discriminatory treatment of Internet traffic allows Internet users to freely disclose the innovation they develop and to offer new applications and services that compete with users already established market players.

In this sense, it is very important to point out that NR policies aim, precisely, at facilitating the empowerment of Internet users, considering them as prosumers.

Therefore, it seems inaccurate to say that the NN policies are in conflict with the interests of the private sector, as argued by some opponents of NN. On the contrary, the policies of NR facilitate the entry of new market players and defend the general interest of the private sector, especially when they are accompanied by other policies that strengthen the openness of the Internet also at the level of the applications and operating systems. In fact, advocates of NN principle include not only human rights supporters, but also a large number of content and application providers and innovators from start-ups *(start-ups)*[169]*.* On the contrary, opponents of NN are generally those telecommunications operators who possess significant market power and defenders of the market's ability to

168 Council of Europe (2010). Declaration of the Committee of Ministers on Network Neutrality. Adopted by the Committee of Ministers on September 29, 2010 at the 1094th meeting of the Ministers' Deputies. <https://wcd.coe.int/ViewDoc.jsp?id=1678287&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021& BackColorLogged=F5D383>.

169 IGF, *supra* note 3, Preamble.

self-regulate perfectly, who argue that Internet access providers must have the freedom to handle traffic. Internet as they please and the regulation of NN could reduce innovation at the network level and prevent the implementation of new business models, such as "*paid prioritization*"[170].

10.2.2 Discrimination or response to the evolution of consumption patterns?

Due to the evolution of Internet consumption patterns[171], in particular the growth of video on demand and games in line, operators have affirmed their willingness to use the ITM to differentiate traffic[172] and propose remunerated prioritization schemes, in order to support the investment[173] which aims to expand the capacity of the network[174].

---

170 The incipient Internet companies *(start-ups)* and those already established have periodically squeezed the adoption of provisions that solidly protect NN in the various countries where NN policies have been discussed. For example, in the EU, the *start-ups* they established the initiative *"Start-ups for net neutrality"*, also replicated in Brazil, while in India almost 700 founders of *start-ups* they have asked Prime Minister Modi to defend the neutrality of the network. *See*, <http://timesofindia.indiatimes.com/tech/tech-news/Nearly-700-startup-founders-urge-PM-Modi-to-defend-net-neutrality/articleshow/50729785.cms>.

171 Wu, Tim and Yoo, Christopher, "Keeping Internet neutral? Tim Wu and Christopher Yoo Debate", in: *Federal Communications Law Journal*, Vol. 59. No. 3, 2007. Available in: <http://bit.ly/2gdkmWW>.

172 While in the nineties, Internet traffic consisted mostly of low bandwidth and a slow e-mail exchange, in the year 2000, the diffusion and download of video with applications *peer-to-peer* began to generate a greater consumption of bandwidth, while the diffusion of *streaming* video and multiplayer high-definition games interconnected simultaneously generalized latency-sensitive applications. See Ou, George, "Managing Broadband Networks: A Policymaker's Guide," The Information Technology and Innovation Foundation (ITIF), December 2008. Available in: <http://bit.ly/1Fz48ui>.

173 The differentiation of traffic is based on the use of any GTI technique "that classifies and applies a potentially different treatment to two or more traffic flows that compete for resources in a network (understand by flow to a group of packages that share a set of properties in common) "BITAG. (2015). "Differentiated Treatment of Internet Traffic." <http://www.bitag.org/documents/BITAG_-_Differentiated_Treatment_of_Internet_Traffic.pdf>. The differentiation is based on the exploitation of multiple traffic classes, which can have different priority levels and can be implemented using differentiated services (DiffServ), integrated services (IntServ) or *multiprotocol label switching* (multiprotocol label switching). *See*, Grossman, D. (April 2002). "New Terminology and Clarifications for Diffserv. Request for Comments: 3260. "April 2002. <https://tools.ietf.org/html/rfc3260>; Baker F., Polk J. Polk and M. Dolly. M. (2010). A Differentiated Services Code Point (DSCP) for Capacity- Admitted Traffic. Request for Comments: 5865. <https://tools.ietf.org/html/rfc5865>; and Rosen et al. Rosen, E. et al. (2001). Multiprotocol Label Switching Architecture. Request for Comments: 3031. "https://tools.ietf.org/html/rfc3031. Unlike traffic *best-effort* (better effort), "traffic intserv or diffserv depends on the differential programming mechanisms in congested routers, with packets of different classes of intserv or diffserv that receive different treatment" (Floyd, S. and Allman, M., "RFC 5290: Comments on the Usefulness of Simple Best-Effort Traffic ", July 2008. Available in: <http://bit.ly/2fqTt0B>.

174 It is important to mention that operators are not the only economic actors that face significant costs and investments. As Felten mentioned, it should not be considered that PCAs take advantage of operators' infrastructure, since they face significant recurrent costs and considerable investments to bring traffic as close as possible to end users (Felten, Benoít, "There's No Economic Imperative to Reconsider an Open Internet ", April 3, 2013. Available in: <http://bit.ly/2ga5dGb>.

The considerable growth of *streaming* of video has required economic efforts to handle the growing demand for traffic[175], thus pressing the operators to propose an extensive use of ITM to establish different prices according to the different quality levels. In this regard, several operators suggested the need for additional fees, in addition to the existing Internet access tariffs, given that, according to the remunerated prioritization schemes, additional income would be obtained to invest in the improvement of the network.

While it is true that NN policies prevent operators from obtaining additional income by implementing paid prioritization offers, it seems unrealistic to say that more revenues would automatically lead to greater investment in infrastructure, or to assume that operators would invest more in infrastructure in the absence of NN frameworks. For example, even though the net profit of the operator Vivo grew 179%[176] during the first quarter of 2016, this operator argued the need to introduce data consumption limits for fixed Internet users in Brazil – as they already exist for mobile Internet users – in order to stimulate investment[177].

In addition, it is important to note that end users pay operators for Internet access and legitimately expect the possibility of accessing and receiving any content, application or service they wish. In this sense, NN intends to prevent network operators from imposing a double price, applying an additional fee to access content, on applications or services that do not have a commercial relationship with operators[178]. In addition, it is essential to mention that the added value of the Internet is the possibility of the user to access, create and share content, applications and services for free. In this way, basing the discrimination of content, applications and services on commercial criteria endangers the very foundations of the Internet: providing an open platform of general use for communication, awareness and innovation.

---

175 Bello, Pablo and Jung, Juan, "Net Neutrality: Reflections on the Current Debate", GCIG Paper No. 13, CIGI and Chatham House, May 2015. Available in: <http://bit.ly/2g9YewV>.

176 OECD. (2014). "The Development of Fixed Broadband Networks". OECD Digital Economy Papers. No. OECD Publishing.

177 *See*, <http://vivo.tl/2eVKTGF>.

178 *See*, <http://bit.ly/2evlnbv>.

In this sense, non-discrimination is essential to allow the circulation of innovation among all users. Most of the commercial actors within the Internet ecosystem are not network operators but web services (with or without profit), *start-ups* or common companies that have an Internet presence: these commercial actors do not have the financial capacity to pay for prioritization schemes, or to practice *zero-rating*, as we will see in the next section, and that is why they have joined the defenders of NN, demanding solid guarantees against discrimination. In this sense, in several countries, the *start-ups* have created coalitions *ad hoc* demanding strong protection from NN[179], and a wide range of Internet companies and technology giants have openly endorsed that "preserving neutrality ensures that the Internet remains a driving force for economic growth, innovation and democratic values[180].

Many of the concerns that emerged in the last decade in the debates about discriminatory treatment are now again emerging in relation to the *Zero Rating*. In fact, the NN policies were adopted in order to avoid operating decisions putting at risk the full enjoyment of the rights of Internet users, while limiting the opening of the Internet. For this reason, it should be noted that opponents of the ZR largely agree with the defenders of NN, while those who support ZR generally agree with the opponents of NN. Next, the evolution of the debate on NN and ZR in the Brazilian context is contextualized.

10.3 The *Marco Civil da Internet* and the regulation of net neutrality and zero-rating

The MCI is the Civil Rights framework in charge of defining the legal basis of Internet regulation in Brazil. Despite its category of ordinary law, the MCI has been considered as the "Internet Constitution"[181] of Brazil, given that it defines the foundational elements of the Internet discipline in Brazil as well as its marked

179 Economides, Nicholas and Tåg, Joacim, "Network Neutrality on the Internet: a Two-sided Market Analysis", in: *Information Economics and Policy Journal*, Vol. 24, February 2012, p. 91-104. Available in: <http://bit.ly/1NCEDyX>.

180 *See*, "Startups for Net Neutrality", available at: <http://bit.ly/2fQwTx3>; "Startups for uma Internet livre", available in: <http://bit.ly/2fL7Jzi>.

181 Internet Association, *supra* note 20.

intention to protect fundamental rights and freedoms *on-line*. The MCI is considered a symbol of participatory democracy due to the online consultation process that led to its creation. The process of opening and collaboration that led to the creation of the MCI was initiated and orchestrated jointly by the Center for Technology and Society of Getulio Vargas Foundation together with the Ministry of Justice of Brazil[182]. Former President Luiz Inácio Lula da Silva promoted the MCI with the commitment to develop a "framework of civil rights for the internet[183]" and received strong support from the also former President Dilma Rousseff who, in response to intelligence revelations by NSA contractor Edward Snowden, called for the implementation of strong guarantees of human rights on the Internet.

Therefore, the MCI was the result of the combination of participatory democracy and the strong political will to protect "freedom of expression, the privacy of the individual and respect for human rights" while guaranteeing the "neutrality of the network, guided only by technical and ethical criteria, its restriction being considered inadmissible for political, commercial, religious or other reasons"[184]. In this sense, the MCI rapporteur in the Chamber of Deputies, Alessandro Molon, argued that NN is a fundamental right and the cornerstone of democracy, which allows individuals to have access to a plurality of information sources[185] .

In this perspective, the consecration of NN in the Brazilian legislation indicates the legislator's understanding that the non-discriminatory treatment of Internet traffic has become a fundamental prerequisite to achieve functioning democracies, driven by the plurality of information, ideas, opinions and innovation. As such the MCI consecrates an obligation to respect net neutrality upon every Internet Access Provider in Brazil, affirming, in its art 9, that:

182 See for example media coverage like TechDirt <https://tinyurl.com/knz42uy or Cnet <https://tinyurl.com/yc5doldv>.

183 *See*, Brazilian Internet Steering Committee (CGI.br), "Um pouco sobre o Marco Civil da Internet", April 20, 2014. Available in: <http://bit.ly/2fQpL3E>.

184 *See* Mário Coelho, "Lula wanted to regulate the internet", *Congresso em Focus,* November 24, 2009. Available in: <http://bit.ly/2eVJ2l3>.

185 *See*, the statement of HE Dilma Rousseff, President of the Federative Republic of Brazil, at the 68th Session of the General Assembly of the United Nations, September 24, 2013.

> The party responsible for the transmission, switching or routing has the duty to process, on an isonomic basis, any data packages, regardless of content, origin and destination, service, terminal or application.

10.3.1 The evolution of net neutrality in Brazil

It is important to note that NN has been defended in Brazil since 2009, when the Brazilian Internet Steering Committee[186], better known by its acronym CGI.br, incorporated NN into its Decalogue of fundamental principles of Internet governance. The decalogue affirmed the importance of NN establishing that "filtering and traffic privileges must be subject only to technical and ethical criteria, being inadmissible political, commercial, religious, cultural or any other form of discrimination or favoritism[187]". This definition was reformulated repeatedly during the process of developing the MCI[188], until its final version was approved in April 2014.

Finally, the net neutrality principle was enshrined in the MCI and imposed "the duty of the operator to process, in an isonomic way, any data packet, regardless of the content, the origin and the destination, the service, the terminal or the application[189]".

Importantly, the MCI explicitly included NN among the principles that define "the discipline of Internet use in Brazil[190]", together with fundamental rights such as privacy and freedom of expression, highlighting the instrumental function of said principles "in order to promote (i) the right of everyone to access the Internet; (ii) access to information, knowledge and participation in cultural life and in the management of public affairs; (iii) innovation and encouragement of the wide dissemination of new technologies and models of use and access[191]". Thus, the MCI assigns NN a

186 *See*, "Molon defends neutrality of the criticism of the Brazilian Internet at the International Conference of FGV-Rio", June 11, 2015, available at: <http://bit.ly/2fQtApt>.

187 The Brazilian Internet Steering Committee is a body that performs several functions aimed at "coordinating and integrating all Internet service initiatives in Brazil and promoting technical quality, innovation and the dissemination of available services". *See*, <http://bit.ly/2fQzIhJ>.

188 *See*, "The principles for governance and the use of the internet". Available in: <http://bit.ly/2fL3jIO>.

189 Ramos, Pedro Henrique Soares, "Arquitetura da rede e regulação: a neutralidade da rede no Brasil", Fundación Getulio Vargas Foundation, School of Law, San Pablo, 2015. Available in: <http://bit.ly/2fPlD1c>.

190 *See*, Civil Framework, art 9.

191 *See*, Civil Framework, art 2.

primary position, placing it among the constitutional principles, in order to highlight the crucial role of net neutrality in promoting a sustainable Internet environment.

The Brazilian legislator has considered that NN is necessary to avoid the type of control that could potentially limit the ability of users to receive and impart information and ideas, including their ability to share innovation. In this sense, the non-discriminatory treatment provided by NN principle multiplies and diversifies the individual's information sources and allows users to become active developers and producers of innovation and content as well as being mere consumers. Thus, a virtuous circle of innovation is unleashed[192], and an equitable playing field is created so that entrepreneurs and companies compete on the basis of the quality of their products and the innovation of their services instead of commercial agreements with operators.

For these reasons, the MCI chooses to firmly protect NN, allowing operators to manage Internet traffic in a discriminatory manner only when such administration is "essential for the adequate provision of services and applications (or for the) prioritization of Internet services." emergency"[193]. Moreover, while the MCI promotes "the freedom of business models[194]" on the Internet, it clearly specifies that such freedom may not exceed NN, stating that commercial offers may not "enter into conflict with the other principles established in this law"[195].

As such, in Article 9, the MCI suggests that practices based on differential treatment should be prohibited. However, because this provision had to be clarified by presidential decree, operators began to offer ZR plans in the Brazilian market, during the elaboration of the decree, arguing that the ZR does not contradict NN and awaiting clarifications by the regulation of the MCI.

192 *Ibid*, art 4.

193 Williamson, Brian, Black, David and Punton, Thomas, "The Open Internet. A Platform for Growth", a report for the BBC, Blinkbox, Channel 4, Skype and Yahoo!, Plum Consulting, October 2011. Available in: <http://bit.ly/2fVt61F>.

194 *Ibid*, art 9.

195 *Ibid* art. 3, VIII.

10.3.2 *Zero Rating*

Usually, the term *Zero Rating* describes commercial practices in which operators, or a third party, sponsor the consumption of data related to a limited number of applications or services, which can be accessed by mobile network users, without incurring expenses for data consumption. Thus, the data consumption of the ZR services is not included in the established data volumes of the users' plans. Occasionally, ZR services can be accessed without the need for a data plan, although in general they are combined with a wide range of data plans. These practices are generally based on positive discrimination of specific applications, and have been proposed in developed and developing countries[196], generating a new wave of debates on NN.

There are several forms of ZR and they can be classified[197] in: (i) ZR of applications; (ii) sponsorship of applications; (iii) ZR platforms; (iv) data sponsorship independent of the applications; v) and sponsored public services[198]. The same provider can offer several ZR schemes in different countries or within the same country. Next, we will briefly analyze the practices of ZR, highlighting the compatibility or incompatibility of the different types of ZR with the foundations of NN. Therefore, the ZR will be considered from the Brazilian perspective.

The majority of ZR schemes aim to achieve two objectives that can be considered fundamental both from the perspective of the operators and the large Internet companies, that is, to attract users – and their personal data[199].

Type of ZR	Who is the sponsor?	What service is sponsored?
Subsidized appliactions	Internet Access Provider	Accesso to apps chosen by the Internet Access provider
App sponsorship	Content or app providers	Access to apps sponsored by CAPs that pay to subsidize access to their apps

196 *Idem.*

197 See <http://www.zerorating.info/>.

198 See Belli, Luca, "Net Neutrality, Zero Rating and the Minitelization of the Internet", in: *Journal of Cyber Policy*, Vol. 2, London, Routledge, 2017.

199 The analysis of this taxonomy is deepened in Belli, Luca, "Net Neutrality, Zero Rating and the Minitelization of the Internet", in: *Journal of Cyber Policy*, Vol. 2, London, Routledge, 2016.

Type of ZR	Who is the sponsor?	What service is sponsored?
ZR Platforms	Potentially Any Entity	Access to apps sponsored by providers or that meet technical requirements imposed by sponsor
Non-discriminatory data sponsorship	Potentially any type of entity	Sponsored data may be used at the discretion of the user
Sponsored public services	Public bodies or Internet Access providers	Access to Public Service Applications

The models featured in the table above present conceptual differences that must be considered in order to understand the passive or active situation of the users, regarding the possibility of choosing how to use their own connection. Such consideration seems essential in order to assess whether or not a business model is compatible with NN's rationale. To facilitate the assessment of the compatibility of the various ZR models with the NN principle, the Body of European Regulators for Electronic Communications (BEREC) has developed criteria[200] that seem particularly useful. These criteria clarify that:

> **41.** A zero-rating offer where all applications are blocked (or slowed down) once the data cap is reached except for the zero-rated application(s) would infringe [net neutrality]

In addition, the BEREC guidelines highlight the existence of practices with anti-competitive effects, pointing out that such practices should be avoided. In particular, BEREC says:

> **42.** The ISP could either apply or offer zero-rating to an entire category of applications (e.g. all video or all music streaming applications) or only to certain applications thereof (e.g. its own services, one specific social media application, the most popular video or music applications). In the latter case, an end-user is not prevented from using other music applications.

200 See BEREC (30 August 2016). BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. BoR (16) 127.

> However, the zero price applied to the data traffic of the zero-rated music application (and the fact that the data traffic of the zero-rated music application does not count towards any data cap in place on the IAS) creates an economic incentive to use that music application instead of competing ones. The effects of such a practice applied to a specific application are more likely to "undermine the essence of the endusers' rights" or lead to circumstances where "end-users' choice is materially reduced in practice" than when it is applied to an entire category of applications

Therefore, to maintain free competition in the market, operators implementing ZR practices should try to subsidize the entire class of applications rather than a specific application with which they have a commercial agreement. In contrast, in most countries where ZR is available, including Brazil, only a few dominant services are subsidized[201] and most Internet application and content providers lack the financial capacity or bargaining power to be included in the plans.

Between the end of 2014 and the beginning of 2016, the Ministry of Justice of Brazil organized a consultation to prepare the decree that regulates the MCI through a participatory process. As in other countries, in Brazil, stakeholders have provided quite polarized responses to the ZR. Interestingly, network equipment operators and manufacturers strongly supported the adoption of ZR models while all the other respondents argued that the ZR should be considered incompatible with the provisions of network neutrality[202]. It should be noted that those who support the ZR argue that this modality would provide consumers with free (i.e. subsidized) access to services, applications and selected content, allowing consumers who do not have resources to access at least some content and services. On the other hand, the detractors of the ZR have declared that, in the long term, the potential benefits of the ZR will appear at the expense of the development of the

201 See the Zero Rating Map available at <http://www.zerorating.info/>.

202 See Belli.

Brazilian digital ecosystem and the freedom of information and opinion of the citizens from Brazil.

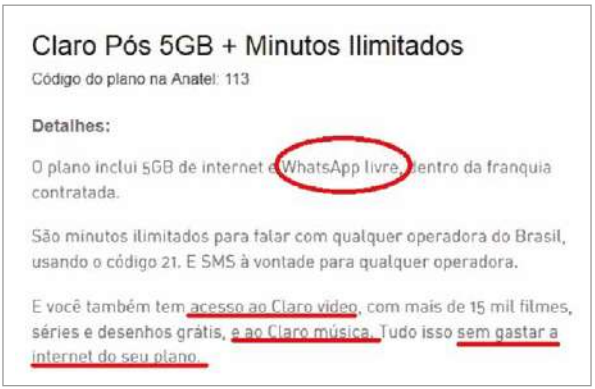
As highlighted above, the most recent data shows that 94.5% of Brazilian mobile users utilize the Internet primarily through instant messaging applications: it is legitimate to ask whether this type of use represents a voluntary choice for Brazilians, or the only option for the most underprivileged. Indeed, this latter segment of Brazilian society mainly use prepaid plans with subsidized message applications. Therefore, it may be argued that, without even realizing it, Brazilians are getting used to using zero-rated services, due to their addiction to such sponsored services, which is purposefully stimulated not only by the addictive nature of the design of these services, but also by the fact they are the only ones perceived as free of charge.

Although the ZR can be considered a legitimate business model, it is important to remember that Article 2 of the MCI requires the strong protection of human rights, plurality and openness of the Internet, and Article 3 explicitly submits "freedom of business models" to the "respect of the other principles established in this law", such as NN. From this perspective, the Brazilian consultation has shown that the ZR intends to guide users towards less expensive services instead of those that are more innovative or useful, thus creating walls that enclose low-income users so that they can only use subsidized services, and predefined by the operators without the possibility of leaving their information bubbles.

The consultation allowed the preparation of decree 8.771/2016[203] that provides a broader guide regarding the illegality of the ZR within the Brazilian legal system. It is noteworthy that Article 9 of the MCI decree prohibits any practice that "compromises the public and unrestricted nature of Internet access and foundational elements and principles as well as the objectives of Internet use in the country" or "favor applications offered by those responsible for the transmission, switching or routing, or by companies of the same economic group."

203 Brito Cruz, Francisco Carvalho et al., "What is at Stake in the Regulation of the Civil Framework?", Final report on the public debate, sponsored by the Ministry of Justice in the regulation of law 12.965 / 2014, InternetLab, 2015. Available: <http://bit.ly/1QZE8kP>.

However, it is important to note that, to date, Brazilian operators have rejected the incompatibility of the ZR and NN, including the services of ZR in a wide variety of data plans. Moreover, it is important to reiterate that, in Brazil, only three dominant social networks – namely: Facebook, Twitter, WhatsApp – together with a very limited number of dominant services and vertically integrated applications are offered through ZR[204]. A clear exemple is offered, for instance, by mobile internet access Claro that, in addition to subsidizing access to WhatsApp, subsidizes its own vertically integrated video and music services.



In this way, the panorama of the ZR in Brazil conclusively exemplifies the critics, according to whom ZR plans are likely to consolidate well-established actors instead of promoting competition, the emergence of new services, and media pluralism. The Brazilian scenario tellingly exemplifies that only the popular and dominant services are attractive enough and have the necessary negotiation power to be included into ZR agreements, and only the applications that are vertically integrated or have commercial parnerships with operators will be zero-rated, despite the fact that such conduct is explicitly prohibited by article 9.3 of Decree 8.771 / 2016.

Moreover, this scenario confirms the critics, according to which ZR ZR has the potential to transform the active users of Internet into passive users of applications, promoting a change from an Internet of general use and generating content to a stagnant network with predefined purpose[205].

204 See Decree No. 8.771, May 11, 2016. Available in: <http://bit.ly/1TRNpKo>.

205 See <http://www.zerorating.info/>.

ZR can be seen as stretegy to efficiently provide and incentivize use of specific application. However, it seems unquestionable that it is based on the positive discrimination of such sponsored services with the aim of encouraging the creation of consumers of specific services instead of free prosumers of the Internet. This evolution seems to be in clear conflict with article 3 of the MCI, which establishes "the preservation and guarantee of net neutrality" as well as "the preservation of the participatory nature of the network" as fundamental principles of the Internet discipline in Brazil. Moreover, by promoting the use of an extremely limited number of subsidized applications, ZR plans do not seem compatible with respect to and promotion of "free initiative, free competition, (...) plurality and diversity" that are explicitly defined in Article 2 of the MCI.

On the Internet, which is a naturally neutral and competitive network, it is possible to develop much more efficient and palatable applications than the dominant social networks, classically sponsored in Latin America and in the majority of developing countries. In an open and competitive environment, it is the creativity and quality of the application that allows to win the competition, not the capability to strike a zero rating deal.

However, one has to undertand that, tragically, an Internet user who is able to create and share new competitive services and to choose them based on their quality and better internet is a risk to dominant players. A free user capable to innovate without permission is a potential competitor. In contrast, a domesticated user whose attention can be directed to zero rated applications and whose personal data can be collected and monetized *ad infinitum* is much more valuable and, above all, much more controllable. This is the main reason why zero rating stratagems are so widespread

10.4 Conclusion

The main foundation of net neutrality is to keep the Internet as an open and decentralized system, whose evolution can be directly modeled by users. As I mentioned, the use of discriminatory ITMs for purely commercial reasons as well as various types of ZR can potentially infringe the basic rationale of NN. In addition, such ZR practices are only useful when combined with data limits

sufficiently low for a consumer to be interested in enjoying the sponsored services. However, the user who develops innovative services and *start-ups* that are not included in ZR agreements will suffer a prejudice due to these practices.

This means that in the absence of data limits, or when data limits are sufficiently abundant, consumers are not inclined to consider ZR offers[206]. In this way, ZR practices can promote artificial shortages, encouraging operators to maintain a low data limit to attract consumers with sponsored services and direct their attention – and the collection of their data – to vertically integrated services with the operator. Although some models of ZR can be used as temporary solutions to allow non-connected individuals to communicate, it is important to note that there are other solutions that may be more sustainable. In particular, public policies should promote full connectivity, giving individuals the power to create and share innovation, and being active prosumers instead of passive consumers. In this regard, policymakers should assess the costs and benefits of the ZR and also consider alternative solutions such as community networks[207].

Community networks are already present in several developed and developing countries and, unlike ZR schemes, are based on individual empowerment through the creation of infrastructure in a decentralized manner, at the user level. Community networks are implemented for the local community that manages them through shared resources and coordinated efforts. This approach is not merely theoretical, but has already demonstrated the ability to produce concrete and distributed benefits. Some featured examples include the Guifi.net network[208] with its more than 33,000 participants scattered throughout the region of Catalonia, Spain, the community

206 Belli, *supra* note 41 The Minitel network was a closed system, especially popular in France during the nineties, in which only the operator could decide what services would be available to users while the French government agency in charge of telecommunications had the right to approve or disapprove any service unilaterally.

207 Arnold, R. et al., "The Value of Network Neutrality to European Consumers", study commissioned by BEREC, April 2015. Available in: <http://bit.ly/2f7apXc>.

208 For a review of community networks, see, Belli L. (Ed.) (2017). Community networks: the Internet by the people, for the people. Official Outcome of the UN IGF Dynamic Coalition on Platform Responsibility. Rio de Janeiro FGV Direito Rio. <http://bibliotecadigital.fgv.br/dspace/handle/10438/19401> Belli (ed.) (2016) Community Connectivity: Building the Internet from Scratch. Annual Rapporteurship of the Dynamic Coalition on Community Connectivity of the IGF. FGV Editor; Baig, R. et al., "Guifi.net, a collaborative network infrastructure", Competer Networks, 2015. Available in: <http://people.ac.upc.edu/leandro/pubs/crowds-guifi-en.pdf.>

networks created by the AlterMundi association in Argentina[209], and the networks developed for the Digital Empowerment Foundation[210]. The main objective of this network is to empower communities through technologies, allowing participants to develop and manage infrastructure as a common resource.

More importantly, community networks allow offering and receiving of any type of service in a non-discriminatory way and without inspection or modification of data flows within the network beyond what is strictly necessary for its operation[211]. As such, community networks are not only compatible with the foundations of net neutrality, but also promote the full empowerment of the user, especially because they are aimed at the population that is not connected. Community networks are based on the use of easy-to-implement network models that individuals who lack technical knowledge can reproduce and exploit in a timely manner[212].

As noted in sections II and III, the practices of *zero-rating* may not be compatible with the neutrality of the network and may substantially limit the way in which individuals can use and take advantage of the Internet. For their part, community networks seem to offer a very concrete response to the search for digital inclusion, given that they not only have the potential to create infrastructure from the ends, but also to stimulate digital literacy, community empowerment and the creation of content and local services. In an era in which governments are frequently criticized for lacking a political vision and prioritizing the interests of well-established private actors, the promotion of sustainable connectivity through user-empowering approaches, such as community networks, would be an intelligent choice to restore the much-needed trust in policymakers, while protecting a non-discriminatory, user-centric Internet.

---

209 See, <http://guifi.net/en/node/38392>.

210 See, <http://docs.altermundi.net/RedComunitaria/>.

211 See, <http://wforc.in/>.

212 Echániz, Nicolás, "Community Networks: Internet from the First Mile", in FRIDA: 10 *Years Contributing to Development in Latin America and the Caribbean*, FRIDA Program, LACNIC, October 2015. Available in: <http://bit.ly/1Nt5aKr>.

10.5 References

ACM. (2015, 27 Enero). Fines imposed on Dutch telecom companies KPN and Vodafone for violation of net neutrality regulations. <https://www.acm.nl/ en/publications/publication/13765/Fines-imposed-on-Dutch-telecom-companies-KPN-and-Vodafone-for-violation-of-net-neutrality-regulations/>.

Agencia IBGE. (2018, 21 febrero). PNAD Contínua TIC 2016: 94,2% das pessoas que utilizaram a Internet o fizeram para trocar mensagens. <https://tinyurl.com/y95fy8qn>.

Arnold, R. *et al.* (2015, Abril) The Value of Network Neutrality to European Consumers. A study commissioned by BEREC. <http://www.wik.org/fileadmin/Studien/2015/2015_BEREC_Summary_Report.pdf>.

Baig, R. *et al*. (2015). Guifi.net, a crowdsourced network infrastructure held in common, Computer Networks. <http://people.ac.upc.edu/leandro/pubs/crowds-guifi-en.pdf>.

Baker, F.; Polk, J. and Dolly, M.(2010). A Differentiated Services Code Point (DSCP) for Capacity – Admitted Traffic. Request for Comments: 5865

Banco Mundial (World Bank). (2016). World Development Report 2016: Digital Dividends. Washington, DC: World Bank

Bauer, J. M. & Obar, J. A. (2014). Reconciling Political and Economic Goals in the Net Neutrality Debate. The Information Society: An International Journal. Vol 30 n°1.

Belli, L. (5 de dezembro 2018). WhatsApp skewed Brazilian election, proving social media's danger to democracy. The Conversation (re-publicado para Business Insider). 5 de dezembro. <https://theconversation.com/whatsapp-skewed-brazilian-election-proving-social-medias-danger-to-democracy-106476>.

Belli, L. (2017). The scramble for data and the need for network self-determination. OpenDemocracy. <https://www.opendemocracy.net/luca-belli/scramble-for-data-and-need-for-network-self-determination>.

Belli, L. (5 de dezembro 2017). Neutralidade de rede e ordem econômica. Observatório do Marco Civil da Internet. <http://www.omci.org.br/jurisprudencia/207/neutralidade-de-rede-e-ordem-economica/>.

Belli, L. (17 de abril 2015). Da neutralidade da rede ao feudalismo na rede. <http://www.brasilpost.com.br/cts-fgv/da-neutralidade-da-rede-a_b_7083750.html>.

Belli, L. (Ed.) (2016) Community Connectivity: Building the Internet from Scratch. Annual Report of the UN IGF Dynamic Coalition on Community Connectivity. FGV Editor.

Belli, L. and De Filippi, P. (Eds.) (2016) Net Neutrality Compendium: Human Rights, Free Competition and the Future of the Internet. Springer.

Belli, L. and Foditsch, N. (2016). "Network Neutrality: An Empirical Approach to Legal Interoperability", in Belli & De Filippi.

Belli, L. and van Bergen, M. (2013). Protecting Human Rights through Network Neutrality: Furthering Internet Users' Interest, Modernising Human Rights and Safeguarding the Open Internet. Council of Europe. CDMSI(2013)Misc19.

BEREC (30 de agosto 2016). BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. BoR (16) 127.

BEREC. (26 de novembro 2012). Differentiation practices and related competition issues in the scope of net neutrality. Final report BoR (12) 132

BITAG. (2015). Differentiated Treatment of Internet Traffic. <http:// www.bitag.org/documents/BITAG_-_Differentiated_Treatment_of_Internet_Traffic.pdf>.

Brito Cruz, F. *et al*. (2015) What is at stake in the regulation of the Marco Civil? Final report on the Public Debate Sponsored by the Ministry of Justice on the Regulation of Law 12.965/2014. <http://www.internetlab.org.br/wp-content/uploads/2015/08/Report-MCI-v2-eng.pdf>.

Cetic.br. (2016). TIC DOMICÍLIOS: Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação nos Domicílios Brasileiros. <http://cetic.br/media/docs/publicacoes/2/TIC_DOM_2016_LivroEletronico.pdf>.

Conselho da Europa. (2014). Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users. <https://wcd.coe.int/ViewDoc.jsp?id=2184807>.

Conselho da Europa. (2016). Recommendation CM/Rec(2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality.

CRTC (29 de janeiro 2015) CRTC continues to set the course for the future of television with Let's Talk TV decisions. <http://news.gc.ca/web/article-en.do?nid=926529>.

Daigle, L. (2015). On the Nature of the Internet. Global Commission on Internet Governance. paper Series n° 7. <https://www.cigionline.org/publications/nature-of-internet>.

Floyd, S. and Allman M. (2008) Comments on the Usefulness of Simple Best-Effort Traffic. Request for Comments: 5290. <https://tools.ietf.org/html/rfc5290#page-3>.

Foro Economico Mundial (WEF). (2011). Personal Data: The Emergence ofa New Asset Class. <http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf>.

Frieden, R. (2014). Net Bias and the Treatment of "Mission-Critical" Bits. 2014 TPRC Conference Paper. Available at SSRN: <http://ssrn.com/abstract=2414149>.

Garcia, J.M., (2016) Network Neutrality and Private Sector Investment. World development report 2016. <http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2016/02/02/090224b08412d57a/1_0/Rendered/PDF/World0developm0te0sector0investment.pdf>.

Grossman, D. 2002. "New Terminology and Clarifications for Diffserv. Request for Comments: 3260." April 2002. <https://tools.ietf.org/html/rfc3260>.

Hart, J.A. (1988). The teletel/minitel system in France. Telematics and Informatics. Vol. 5. N° 1.

Haucap, J. and Heimeshoff, U. (2013). Google, Facebook, Amazon, eBay: Is the Internet Driving Competition or Market Monopolization? DICE Discussion Paper n°83. <http://www.dice.hhu.de/fileadmin/redaktion/Fakultaeten/Wirtschaftswissenschaftliche_Fakultaet/DICE/Discussion_Paper/083_Haucap_Heimeshoff.pdf>.

IDEC. (15 de abril 2016) Idec entra na Justiça para barrar limite à banda larga fixa. <http://www.idec.org.br/em-acao/em-foco/idec-entra-na-justica-para-barrar-a-banda-larga-fixa>.

IGF. (2015a). Policy Statement on Network Neutrality. Outcome of the 15th United Nations Internet Governance Forum. <http://www.intgovforum.org/cms/documents/igf-meeting/igf-2016/833-dcnn-2015-output-document/file>.

IGF. (2015b). Paper on the work of the Dynamic Coalition on Core Internet Values. Outcome of the 15th United Nations Internet Governance Forum. <http://www.intgovforum.org/cms/documents/igf-meeting/igf-2016/824-dcciv-2015-output-document/file>.

ISOC. (2012). The Internet and the Public Switched Telephone Network: Disparities, Differences, and Distinctions. <https://www.internetsociety.org/sites/default/files/The%20Internet%20and%20the%20Public%20Switched%20Telephone%20Network.pdf>.

Mirani, L. (2015). Millions of Facebook users have no idea they're using the internet. <http://qz.com/333313/milliions-of-facebook-users-have-no-idea-theyre-using-the-internet/>.

Nam, H. (2015). Killing Network Neutrality – Massive Blocking P2P Traffic by KT Corporation. <http://opennetkorea.org/en/wp/1529>.

Organização para a Cooperação e Desenvolvimento Económico (OCDE). (2013). Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value. OECD Digital Economy Papers, No. 220. OECD Publishing. Paris. <http://dx.doi.org/10.1787/5k486qtxldmq-en>.

Ouvidoria da Anatel. (2016). Relatório Analítico: Agosto 2016. <http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=343764&pub=original&filtro=1&documentoPath=343764.pdf>.

Rosen, E. *et al.* (2001) Multiprotocol Label Switching Architecture.

Request for Comments: 3031. <https://tools.ietf.org/html/rfc3031>.

Silverman, A. (22 de novembro 2016) The Top Fake News Stories Outperformed Real News About A Major Scandal In Brazil, Too. <https://tinyurl.com/y7nv7j7p>.

Wu, T. (2003). Network neutrality, broadband discrimination. Journal of Telecommunications and High Technology Law, 2, 141.

Wu, T. and Yoo, C. (2006). Keeping Internet neutral?: Tim Wu and Christofer Yoo Debate. Federal Communications law journal. Vol 59. N° 3.

A SUSTAINABLE EXPANSION OF CONNECTIVITY

11 Community Networks and the Principle of Network Self-determination

Luca Belli

Note: this article is based on the content previously published in Luca Belli (Ed.) (2017). Community networks: The Internet by the people, for the people. Official Outcome of the UN IGF Dynamic Coalition on Community Connectivity. Rio de Janeiro: FGV Direito Rio. Pp 35-64.

Abstract

This article argues that any individual should enjoy the right of "network self-determination" and that such a principle, despite not being recognized yet *de jure,* is already being implemented *de facto*, thanks to the development of community networks. Community networks are digital network infrastructures based on collaboration and are established in a bottom-up way for the members of the local communities that develop and manage the network infrastructure as a common asset. The self-determination of the network, as far as it is concerned, should be considered as the right to associate freely, in order to define, democratically, the design, development and management of the community network infrastructure, in order to search, transmit and receive information and innovations freely. The first section of this article argues that the principle of network self-determination finds its conceptual bases in the fundamental right to self-determination of people, as well as in the right to informational self-determination. The study emphasizes that the self-determination of the network plays a fundamental role, allowing individuals to associate and join efforts to overcome digital gaps in a collaborative manner. In this perspective, the second section of the article examines a selection of community networks, highlighting the positive externalities unleashed by such initiatives that favor the establishment of new participatory governance structures and the development of new content, applications and services that meet the needs of the communities, empowering previously disconnected individuals. The study offers evidence that the development of community networks can induce several benefits, creating learning opportunities, stimulating local entrepreneurship, promoting the

creation of new jobs and reinvigorating the social connections of communities, through multi-stakeholder associations, which bring local institutions closer to business owners and community members.

11.1 Introduction: A bottom-up response to the lack of connectivity

Community networks are based on collaboration and are developed in a *bottom-up* fashion by the members of the communities that construct and manage the Internet infrastructure as a common good. The debate on community networks offers a solid demonstration of how Internet governance processes allow multiple *stakeholders* to self-organize, in order to achieve common goals and how such multistakeholder cooperation can concretely influence the evolution of the Internet. Despite the fact that community networks have been analyzed for more than twenty years, they entered the international policy arena mainly due to the Internet Governance Forum (IGF) and the platform for visibility and organization it offers, particularly thanks to the possibility to create working groups dedicated to specific topics, called Dynamic Coalitions[213]. The potential of these groups is often underexploited but they play an incredibly important function, allowing individuals and entities interested in a common theme to associate and organize with continuity and eventually develop participatory "principles, rules, decision-making procedures and shared programs that shape the evolution and use of the Internet"[214].

In this sense, since the creation of the Dynamic Coalition on Community Connectivity[215] (DC3), a growing number of individuals and organizations from around the world started to coordinate to organize joint actions, produce research and elaborate or share

213 For an analysis of how dynamic coalitions can be considered as collaborative and Habermassian instruments oriented towards the elaboration of digital policy proposals, see Belli (2016a), pp. 368-374.

214 Such activities constitute the definition of Internet governance, according to the Tunis Agenda for the Information Society, adopted by the World Summit on the Information Society of the UN in December 2005. See <http://www.itu.int/net/wsis/docs2/tunis/off/6rev1-es.pdf>.

215 DC3 was created as a result of the first workshop that analyzed community networks in the framework of the IGF in 2015. See Workshop 223 "Community Networks: a Revolutionary Paradigm" <http://sched.co/4c19>.
For additional information on DC3, see www.comconnectivity.org and www.tinyurl.com/ IGFDC3.

public policy suggestions aimed at making more visible[216] the potential that community networks have as a concrete solution to overcome existing digital divides[217]. One of the products developed by DC3 is the Declaration on Community Connectivity, which was developed through a multistakeholder participatory process. The process began with an open online consultation, between July and November 2016, continued with a public debate and a process of feedback collection, during the 2016 IGF, and ended with a further online consultation, between December 2016 and March 2017[218]. The Declaration represents the first example of an international consensus document on the characteristics of community networks, their users, and the public policy elements that can facilitate such networks.

According to the Declaration, community networks are "structured to be open, free and respect the neutrality of the network. These networks depend on the active participation of local communities in the conception, development, implementation and management of shared infrastructure as a common resource, owned by the community and operated in a democratic manner."[219] These community-driven networks give rise not only to new infrastructures, but also to new governance models and new business opportunities and access to information to fill the gaps left by the "traditional"[220] paradigm of provision of Internet access.

In fact, the traditional paradigm of Internet access provision, where operators develop and manage network infrastructure in a *top-down* fashion[221], presents some clear limitations that are expressly

216 In this sense, it is sufficient to analyze the programming of the main events on Internet governance, such as the IGF, the ITU WTDC, RightsCon, EuroDIG, etc. – as well as the sponsorship programs of projects of organizations such as Mozilla, ISOC, RIPENCC, APNIC, etc. to verify the appearance and the considerable diffusion of the topic of the community networks in agreement with the establishment of the DC3 from the end of 2015.

217 For an analysis of existing digital obstacles, World Bank (2016); ITU (2016a).

218 See the Statement on Community Connectivity <https://comconnectivity.org/article/dc3-working-definitions-and-principles/>.

219 *Ibid.*

220 In the present article, the expression "traditional paradigm of provision of Internet access" refers to the Internet access model based on the existence of a network operator that provides access to a plurality of subscribers. In accordance with RFC 7962, the expression "traditional networks" or "*mainstream network*" denotes generally large networks that cover large areas; they are controlled in ascending order by the operator; they require a substantial investment to be built and maintained; and do not allow user participation in the design, implementation, operation, governance and maintenance of the network. (Saldana *et al.*, 2016: 5).

221 *Ibid.*

exemplified by the almost 4 billion individuals[222] that until now are still disconnected from the Internet. Therefore, the emergence and diffusion of community networks represents a spontaneous reaction of the populations that are directly interested by the various existing digital divides.

In many rural areas and in the peripheries of many metropolises, population is scarce and individuals have significantly lower living standards than the average. For these reasons, operators neglect the expansion of network infrastructure in these areas, due to the insufficient return on investment. The aforementioned areas are indeed commonly referred to as market-failure areas because, as the definition tellingly suggests, the market fails to connect them. Thus, the traditional model of provision of Internet access, driven by the investments of telecommunications operators, cannot be considered as a universal and infallible solution because, although it can efficiently provide connectivity to urban and rich populations, this model clearly needs to be complemented with different approaches to meet the needs of a more diversified public. It is clear that the approach driven by the demands of the market can face two types of failures in rural and peripheral areas:

- The prospect of a lost return on investment can lead to a lack of coverage, or a quality of service so low that potential or existing users may be discouraged from using available offers of Internet access;
- Due to lack of competition, Internet access offers can be prohibitively expensive for most low-income areas, where people may need to sacrifice food in order to afford communication[223].

In addition to the elements mentioned above, many individuals may not perceive the interest of Internet connectivity because the services and content they would need, such as local e-government services, e-commerce, digitized health services, and local content, are not available online.

222 For a precise estimate, compare the number of global Internet users and the world population in <http://www.internetlivestats.com/internet-users/> and <http://www.worldometers.info/world-population/>.

223 See Rey-Moreno *et al*. (2016).

The emergence of community networks is a concrete response to these situations, with the objective of truly empowering the disconnected, allowing individuals and communities to self-determine, enjoying all the opportunities that connectivity can offer, at the same time as connected individuals they contribute to the generation of even more services, contents and opportunities. In this sense, users of community networks fully enjoy the fundamental characteristic of each Internet user of being a "prosumer", being not only a consumer of content but also having the possibility of being a producer of new potentially disruptive applications and services., which meet the needs of local communities and compete freely with established market players.

As will be argued in the second section of this article, the analysis of community network initiatives provides a concrete basis for the promotion of the right to self-determination of the network, which can be exploited through the establishment of new infrastructure, creating new opportunities socio-economic and actively participating in the evolution of the Internet as well as the socio-economic evolution of its local community.

Therefore, the thesis of this article is that groups of individuals who experience firsthand the effects of digital obstacles, as well as any other individual, have the right to the development of network infrastructure. In this sense, the self-determination of the network should be considered as an instrumental condition to allow the full exercise of the human rights of the people and as a fundamental principle of Internet governance. Network Self-Determination can be enjoyed when individuals enjoy the possibility of freely associating and defining, democratically, the design, development and management of new infrastructures, as a common good, that allow them to interconnect and search, transmit and receive freely information and innovations.

11.2 The right to Network Self-Determination

This section will argue that the right to network self-determination finds its conceptual and legal bases in the fundamental right to

self-determination of people[224], well as in the right to "informational self-determination"[225] that since the 1980s began to be consecrated as an expression of the right to the free development of personality. The present study will emphasize that the self-determination of the network plays a fundamental role, allowing individuals to associate with collective entities, joining forces to overcome digital obstacles in a participatory and *bottom up* manner.

In this perspective, the self-determination of the network directly impacts the participatory and sustainable development of the Internet ecosystem. To corroborate this thesis, the second section of the article will examine three examples of community networks, highlighting the positive externalities unleashed by such initiatives in terms of the establishment of new structures of participatory governance, as well as the development of new content, applications and services that meet the needs of local communities, empowering previously disconnected individuals and creating new opportunities.

The ultimate goal of community networks is the economic, social and cultural development of local communities, in the terms established democratically by these communities. In this perspective, one of the main characteristics of community networks is to adapt to the needs of the communities at the origin of such initiatives and, sometimes, the members of these communities can decide not to connect to the Internet, but to build local intranets that are they will connect to the Internet only sporadically. In some other cases, members of the community may even decide to structure the new infrastructure based on radio technology, such as the Fonias Juruá network[226] in the Brazilian Amazon, instead of exploring networks based on the Internet protocol. These considerations are very important if we consider connectivity in terms of self-determination and community networks as an expression of such self-determination.

---

224 This fundamental right is enshrined prominently in Article 1 of the Charter of the United Nations, as well as in Article 1 of the International Covenant on Economic, Social and Cultural Rights and the International Covenant on Civil and Political Rights.

225 See the decision "Census" of the German Constitutional Court of December 15, 1983 BVerfGE 65, 1-71, Volkszählung.

226 See Antunes Caminati *et al*. (2016).

11.2.1 The fundamental right to self-determination of peoples as a basis for network self-determination

The fundamental right to self-determination plays an instrumental role in enabling individuals to enjoy their inalienable human rights and, therefore, is enshrined as the first article of the Charter of the United Nations and both International Covenants on Human Rights. In accordance with these instruments of international law, the states agreed that "all peoples have the right to self-determination" and that "by virtue of that right, they are free to determine their political status and pursue their economic, social and cultural development." Article 55 of the Charter of the United Nations corroborates the aforementioned provisions, imposing on the Member States of the UN to generate stability and well-being "on the basis of respect for the principle of equal rights and self-determination of peoples", while Article 1 (3) of both Covenants obliges the signatories to "promote the realization of the right to self-determination." Although such provisions have been interpreted, in a postcolonial context, as the right to territorial separation of each ethnic, linguistic or religious group, it is not the interpretation on which this article is based to propose the construction of the right to network self-determination. On the contrary, this article argues that network self-determination must be associated with the interpretation of the right to self-determination as a collective right of a community to determine its own destiny, promoting socio-economic development and self-organization.

It should be reiterated that network self-determination should not be linked to territorial separation, but to the essence of the right to self-determination as the right pertaining to every people, allowing to self-determine the most appropriate governance system, which is formally recognized by binding instruments of international law.

When it comes to connectivity, this means having the possibility to project and organize in an independent and democratic way the network infrastructure that will allow the members of a community to interconnect. In this perspective, we must consider the development of community networks not only as a concrete strategy to expand connectivity, but also as a laboratory for new

structures of participatory governance that allow the transposition of democratic organizations from local communities to the governance of the electronic networks that provide connectivity to these communities.

Thus, the self-determination of the network allows building a direct bridge between fundamental rights and Information and Communication Technologies (ICT) through connectivity. As such, connectivity must be considered as an essential condition to fully enjoy freedom of expression and, in turn, in the digital sphere, freedom of expression – which is the fundamental right to seek, transmit and receive information and ideas without Interferences – should be considered as the right of each individual to access, develop and share content, applications and services, without interference.

In addition, it is important to emphasize that the right to communicate should not be considered an obligation to connect with the rest of the world permanently or as an obligation to use a specific type of technology or predefined applications chosen by third parties. On the contrary, individuals must have the right to determine autonomously how they want to build and organize the network infrastructure that allows them to improve their economic and social situation and improve their political organization, independently deciding what types of technology, applications and content are the most important, most suitable to meet the needs of the local community. This possibility is essential for people who live in areas where operators have no return on investment and, therefore, community networks should be considered as a need rather than an option. As such, network self-determination must be addressed in terms of economic and cultural autonomy, which is essential to promote human rights and dignity for each individual and group of individuals.

Those responsible for public policy should also consider the relevance of this last point, when deliberating on how Universal Access Funds should be used. These funds could have a considerable impact if they are used, at least in part, to support the establishment of community network initiatives rather than being

wasted through inefficient subsidies or for "unknown purposes[227]" as it happens excessively often. In this perspective, governments should try to devote at least a fraction of the financial resources collected under the Universal Access Funds to programs that provide plants to organizations or individuals that present solid plans for the development of community networks.

11.2.2 Informational self-determination as the foundation of network self-determination

The second conceptual basis for the self-determination of the network can be found in the "right to informational self-determination", which was first declared by the German Constitutional Court. In 1983, the German Supreme Court explicitly recognized the individual right to "informational self-determination" as an expression of the fundamental right to have and develop a personality enshrined in Article 2.1 of the German Federal Constitution. It is important to highlight that this last right is also formally recognized internationally. Article 22 of the Universal Declaration of Human Rights affirms that "everyone has the right to the realization of the necessary rights to dignity and to the free development of his personality", while the International Covenant on Economic, Social and Cultural Rights consecrates that fundamental principle in relation to the right of everyone to education and to participate in public life, foreseeing that the right to education "must be directed to the full development of the human personality and the sense of its dignity [...] and allow all people to participate effectively in society "(article 13.1) and considering the free development of the personality as an instrumental element to exercise the fundamental right to "participate in cultural life [and] take advantage of the benefits of scientific progress and its applications" (article 15). Since the eighties, the right to informational self-determination has become a cornerstone of the protection of personal data. In fact, the reasoning of the German Court stressed that the right to informational self-determination

227 In Brazil, for example, universal access funds collected between 2001 and 2016 totaled approximately US $ 7 billion, but, according to the Court of Accounts of the Union, only 1% was used for universalization programs, while 79% for "unknown" purposes. See: <http://convergecom.com.br/wp-content/uploads/2017/04/Auditoria_TCU_fundos.pdf>.

holds "the individual's ability to determine the disclosure and use of their personal data"[228], thus assigning individuals the right to choose which personal data may be disclosed, to whom and for what purposes they may be used. This principle is the basis of the rules that delineate the right to data protection in the national legal systems of 120 countries[229], including several Member States of the Organization of American States[230].

It should be noted, however, that over the last twenty years the collection, processing and sale of personal data have become the main source of income for most Internet services, challenging the exercise of informational self-determination of connected individuals. In fact, the business models of most services and applications depend mainly on the collection and monetization of user data. Although these business models denominated "zero price" present the services as "free", it is widely recognized that users pay the price in fact with their personal data, which are collected and monetized for various purposes, such as direct mail[231]. This is precisely the reason why, in the last decade, authors and institutions emphasized that "Data is the new oil"[232] and represents a "new asset class"[233] and that personal data should be considered as "the new currency of the digital world"[234] and "the most valuable resource in the world"[235].

Despite these considerations, most users do not perceive the value of their personal data or the fact that these data represent the price of the online services they access "for free." In addition, the vast majority of users do not understand the implications of the collection and processing of their personal data, accepting the terms of use of services without reading them to take advantage of

228 See BVerfGE, paragraph 65.1.

229 See Greenleaf (2017).

230 See <http://www.oas.org/es/sla/ddi/proteccion_datos_personales_dn.asp>.

231 For a comprehensive analysis of how Internet companies collect, combine, analyze and market personal data of individuals, see Christl (2017).

232 The phrase was coined by British mathematician Clive Humby in 2006 and subsequently popularized by the 2011 World Economic Forum report on personal data. See WEF (2011).

233 *Ibidem.*

234 See Kuneva (2009).

235 See The Economist (2017).

the supposedly "free" services[236]. In this context, it is important to point out that, in the last five years, the logic of the model of *zero price* has been applied to Internet access plans, sponsoring limited access to specific applications, presented as "free" because their data consumption is not discounted from users' monthly franchises. In fact, the personal data of individuals have become such a valuable asset that companies are available to sponsor access to specific applications – usually provided by business partners[237] – to collect and use the data produced by the (new) users of said applications.

The aforementioned offerings are generally classified as "*zero rating*"plans[238] and are presented by some *stakeholders* as a strategy to "connect the disconnected[239]. "However, it should be noted that, despite of rhetoric, the goal of most of these offers is not philanthropic, but it is guiding the user experience for predefined applications[240], whose access will be paid by users, rather than with money, with their "free work"[241] as data producers and with their resignation to be a prosumer that could potentially develop, and freely share, new services that compete with the sponsored services.

In light of these considerations, for a corporation that has the economic capacity and sufficient bargaining power, it seems strategic to sponsor access to its applications, in order to obtain a resource as valuable as personal data and, at the same time, create an impediment for competitors who do not have the same bargaining power and financial capacity. This reasoning is particularly relevant when it comes to developing countries, where personal data represent a totally unexplored resource because a considerable proportion of the population is still disconnected, and local developers do not have the economic conditions to sponsor

236 For a critical perspective on the notice and consent model and a proposal for a user-centered data management model, see Belli, Schwartz and Louzada (2017). It should be noted that most users ignore that their personal data are used to monitor their behavior in real time and to make very sensitive decisions, such as assessing the solvency in case of loan request based on their digital behavioral data, as highlighted by Christl (2017).

237 For a panorama that applications are sponsored in the world, see <http://www.zerorating.info/>.

238 For an analysis of the practices of *zero rating*, see Belli (2016c).

239 This motto is particularly used by the private sector (GSGA 2016), but it was also integrated by local institutions, such as ITU. For example, ITU (2017).

240 I define this phenomenon as "Minitelização de la Internet." See Belli 2016c and 2017.

241 For an analysis of the value produced by users' free work of use, see Beverungen, Böhm and Land (2015).

access to the services themselves. In this sense, zero rating plans have been criticized as being a form of discriminatory treatment contrary to the principle of net neutrality[242] and, also, to represent a form of "digital colonialism"[243] in the realm of a "run towards data"[244] focused on sponsoring applications in order to drain "the most valuable resource in the world."

On the contrary, as I will highlight in the next section, community networks promote the self-determination of the network, since they are based on an active user's position and allow individuals to autonomously decide how to pursue their economic, social and cultural development. The objective of community networks is, in fact, to train individuals who become new active participants of the Internet, taking advantage of the benefits of connectivity and contributing to the evolution of the Internet in a *bottom-up* manner. Many examples[245] in different formats demonstrate that, in addition to being a viable option, community networks can be scalable and unleash a wide range of positive externalities for local communities, improving digital literacy and access to knowledge, as well as the production and circulation of content and local services, and reviving or even creating local economies.

Thus, these initiatives play an important role in the promotion of network self-determination, promoting freedom of expression and association and strengthening informational self-determination, because users are not obliged to exchange their personal data for access to sponsored services, but stimulated to develop new services for the local community. This last point explains in a crucial way the relevance of community networks, which can effectively empower previously disconnected communities.

11.3 Positive externalities of the community network

Participants in community networks know that they contribute positively to the local socio-economic environment, creating

242 See analysis of the challenges of net neutrality, see Belli & De Filippi (2016) and <http://www.networkneutrality.info/>.

243 Consult Chakravorti (2016); Shearlaw (2016).

244 See Belli (2017c).

245 See eg Belli (2016b e 2017b).

learning opportunities, establishing efficient social organizations and stimulating local entrepreneurship[246]. In particular, in addition to providing access to information and knowledge, these networks focus specifically on the needs of their users, stimulating the development and offering of services adapted to the local community. In this sense, the participants of many community networks developed a variety of tools aimed at organizing community life more efficiently, such as maps or shared planning tools, as well as offering messaging applications, local e-commerce platforms, social networks, broadcasting and video broadcasting. Therefore, these initiatives have the potential to reinvigorate local economies and the participation of the community in local politics and administration. In this perspective, it is even more interesting to evaluate the possible benefits that community networks can implement in relation to the local economy, with special attention to the promotion of employment opportunities for local populations.

Next, four case studies are analyzed, highlighting some of the elements that contribute to the success of community networks and some challenges that these initiatives commonly face.

11.3.1 Guifi.net

Guifi.net is the largest community network and probably the most famous and most studied example of community networks[247]. Guifi.net was founded in 2004, in the Municipality of Osona, in Catalonia, Spain, with the objective of solving the difficulties of Internet access in rural areas, due to the reluctance of traditional operators to implement their networks in such regions[248].

Note that Spain is categorized as an advanced economy[249] and, in 2016, it was ranked 26th out of 174 members of the International Telecommunication Union (ITU) by the GlobalICTsDevelopment Index[250]. These elements are particularly important to understand the context in which Guifi.net was developed, but also that the

246 *Ibid.*

247 For an analysis of Guifi.net, see *Baig et al.* (2015) e Baig *et al.* (2016).

248 Consult <https://guifi.net/en/what_is_guifinet>.

249 See *eg* IMF (2017), according to which the Spanish GDP per capita 2016 was US $ 27,012.

250 See ITU (2016: 12).

focus of the community network is not limited to developing countries, but, on the contrary, it has very specific applications in practically all countries including developed ones. Guifi.net currently covers a broad area and reached about 85,000 users that can be grouped into 34,000 active nodes, with typically 2.5 users per node[251]. As in many community networks, each node corresponds to a house, which generally has 2.5 inhabitants in the areas covered by Guifi.net. In addition to being the largest and most populated community network in the world, Guifi.net is also notable due to the large number and variety of services[252] that its members developed and used regularly.

The idea of the founders of Guifi.net was to build a network infrastructure as a common good, to be exploited in a fair, sustainable and scalable way. This idea favored the establishment of a disruptive economic model based on the model of the common goods and the collaborative economy[253]. As noted by Baig *et al*. (2015:153) Guifi.net's cooperative model is the reason why new entrants, and small local businesses can easily develop and share new services, given the reduction in entry costs and the reinvestment of initial investments. Among the wide range of services developed by Guifi.net members, it is worth mentioning:

- 8 direct Internet gateways and 306 proxies;
- 48 Web servers;
- 31 file transfer protocols or shared disk servers;
- 13 Voice over IP communication services (*Voice over IP*);
- 13 transmission radios;
- 6 instant message servers and 7 Internet Relay Chat servers;
- 5 videoconferencing servers;
- 4 e-mail servers.

In addition, one element that regulators should pay attention to is the fact that initiatives such as Guifi.net can be job creators:

251 In a communications network, a node is a connection point that can receive, create, store or send data through distributed network routes. See <http://searchnetworking.techtarget.com/definition/node>.

252 A complete list of services developed by the Guifi.net community can be found in <https://guifi.net/node/3671/view/services>.

253 See <https://guifi.net/en/what_is_guifinet>.

entrepreneurs and local developers can develop and offer new services, while the new network needs to be maintained by a team of professionals. Thus, the mere establishment of a community network will create jobs at least in relation to its maintenance. In this perspective, Guifi.net offered employment to 37 "certified professionals" and 13 installers not professionally registered (that is, not full time). It is interesting to note that certified professionals can be individuals or small and medium enterprises: therefore, the effective number of people employed is several dozen, because each certified company can employ up to 10 individuals.

Figure 1: Location of the nodes in July 2016[254].

Thus the creation of community networks has the potential not only to provide connectivity to previously disconnected communities, but also to revive local economies, promote the creation of entirely new jobs, services and business opportunities. In addition, these initiatives generally involve cooperation among their members and local institutions, such as local administrations, libraries, schools or universities. The Guifi.net case is also emblematic on this point, having established cooperation with hundreds of local institutions

254 See Baig *et al.* (2015).

that cooperated in the establishment of an effective governance mechanism that, as pointed out by the Elinor Ostrom (1990), is fundamental for a sustainable management of common long-term resources. The definition of a solid governance structure is one of the main ingredients for the success of community networks, as indicated in the Conclusions.

11.3.2 Nepal Wireless Networking Project

The *Nepal Wireless Networking Project* (NWNP) was established in 2002, with the original purpose of providing Internet access and telephony services to Himanchal Higher Secondary School, in the Nepali district of Myagdi (Pun *et al.* 2006). Unlike the Guifi.net example, the NWNP is in one of the poorest and least developed countries in the world. In fact, Nepal has an extremely high unemployment rate[255] and ranked 142nd out of 174 ITU members for the 2016 ICTs Global Development Index[256]. In this context, initiatives aimed at increasing connectivity for the benefit of local populations have the potential to drastically improve the living patterns of affected communities.

Shortly after the creation of the NWNP, the founder of this community network, Mahabir Pun, decided to set more ambitious goals, with the aim of covering the digital deficiencies starting from the "closest level of the population"[257] and, over the years, the NWNP has become a social enterprise dedicated to bringing the benefits of wireless connectivity and ICTs to populations living in several mountainous areas of Nepal. Mahabir Pun's vision was to consider connectivity as a propellant for the socioeconomic development of local communities and in this sense combined the development of infrastructure with the organization of training programs and with the development of services that could respond to the needs of the populations.

255 See the World Bank's overview of Nepal <http://data.worldbank.org/country/nepal#cp_wdi>.

256 See ITU (2016: 12).

257 See Pun *et al.* 2006.

Figure 2: NWNP tower is installed in a Nepalese peak of the Himalayas[258].

The integrated approach, adopted by the NWNP, considered the positive externalities of connectivity *ab initio*, developing wireless infrastructure with the explicit objective of going beyond the sale of Internet access signatures. In this perspective, the objective of the NWNP is the sustainable empowerment of the local community through five fundamental objectives[259].

- Allow stable communications in the less accessible areas of Nepal through the provision of Voice over IP services, email applications and the organization of a Nepali language electronic bulletin, facilitating community discussions, while promoting new forms of communication and electronic governance;
- Increase educational opportunities for members of the local community, through the establishment of distance learning and training programs aimed at overcoming the lack of qualified teachers in rural areas, and creating local intranets that allow access and sharing of pedagogical material;
- Allow access to quality medical care, providing telemedicine programs and remote medical assistance. This point was implemented in association with various hospitals;
- Promote e-commerce, allowing community members to sell local products, creating an online version of local markets;

258 See <http://www.nepalwireless.net/index.php>.

259 See Pun *et al.* (2006: 5-7).

- Generate jobs with special attention to younger generations, thanks to the availability of training programs in local telecentres.

It seems unnecessary to say that this integrated approach is precisely what makes community networks, or any other connectivity strategy, successful. Regulators should simply base their strategy on the basis of the points mentioned above to wisely use Universal Access Funds. In particular, the NWNP proved to be particularly successful due to the incredible number of start-ups it generated throughout its 15 years of life. Several social enterprises in areas such as electronic agriculture, the supply of medical content and intelligent environment services were developed thanks to the ecosystem established by the NWNP, improving the living standards of thousands of individuals. For example, members of local communities regularly explore the application of Haatbazar electronic agriculture to organize agricultural activities, such as the creation of herbs and the production of cheeses, while local farmers have used NWNP to sell livestock and access veterinary material updated.

In addition, to stimulate the use of ICTs by women, the NWNP team began to develop content related to pregnancy that could be easily shared via SMS. This strategy was so successful in promoting the acceptance and use of technology by women that an Android application, called Amakomaya, was developed to provide medical information for pregnant women through smartphones. Finally, several weather stations are connected to the NWNP to provide updated weather information to local communities, helping to improve the local system of surveillance against poachers, developed by the members of the NWNP to monitor the Chitwan National Park, thus protecting several species extinction threats.

11.3.3 Telecomunicaciones Indígenas Comunitarias Asociación Civil

Telecomunicaciones Indígenas Comunitarias Asociación Civil5[260] (TIC-AC) is an institution managed by the NGO Rhizomatica[261].

260 See <https://www.tic-ac.org/>.

261 Founded in 2009, Rhizomatica aims to make the alternative telecommunications infrastructure possible for people around the world. See <https://www.rhizomatica.org>.

Rhizomatica's work consists in the creation and promotion of technology in open access that helps people and communities to build their own networks. At the same time, Rhizomatica develops and promotes governance strategies to implement the sustainable development of community networks. TIC-AC was founded in 2013 and thanks to its successful example, the possibility of establishing community networks in Mexico was institutionalized some years later, by virtue of Decision 73/2016[262] of the Federal Institute of Telecommunications of Mexico. This decision created the first license for telecommunications service for indigenous social use, allowing the installation of community networks, based on GSM technologies, in the Mexican states of Oaxaca, Chiapas, Veracruz, Guerrero and Puebla. The decision was hailed as a historic resolution, being the first formal act in the world that institutionalized a telecommunications license for indigenous social use"[263].

Figure 3: Location of the communities connected by TIC-AC.

Although Mexico is considered an emerging market[264] and, currently, occupies the 92nd place among the 174 members of the ITU by the ICTs Development Global Index[265], it is important to note that the state of Oaxaca, where the TIC-AC is established, is

262 See Communication 73/2016 <http://tinyurl.com/ycjx3awj>.

263 Although Communiqué 73/2016 is the first regulatory asset to officially adopt the term "indigenous social use license", it should be noted that the Kuh-ke-nah (K-Net) network, in the province of Ontario, Canada, was pioneer in the development of community networks to connect indigenous communities, since 2001. See <http://grandopening.knet.ca/>.

264 See, for example, IMF (2017).

265 See ITU (2016: 12).

among the least developed in the Mexican federation[266]. Oaxaca is in southern Mexico and is known for its more rugged terrain, with mountain ranges, narrow valleys and canyons. This orographic configuration, together with a low population density, has traditionally been considered as an obstacle to the implementation of the telecommunications infrastructure. On the other hand, the same factors helped to preserve the indigenous culture, making the population of the state one of the most diverse in the country, representing 53% of the indigenous language population of Mexico. In this context, the dual purpose of TIC-AC is to provide connectivity while allowing local populations to self-determine how their network infrastructure should be organized and used to meet their needs and allow sustainable development.

TIC-AC is based on GSM technology that offers communication services to about 3000 users. Among the services developed by the ICT-AC community, Voice over IP applications are probably the ones that have the greatest impact, allowing community members to communicate, organize and maintain contact with family members migrated abroad, paying a small fee fraction of the price previously necessary to make national and international calls. The project is executed by a team of nine individuals and supported by another 20, who are employed as managers of the 20 networks that make up the TIC-AC. In this regard, it should be noted that, in addition to allowing connectivity, TIC-AC also created 29 direct jobs for the local community. The project was so successful that other civil society actors replicated it spontaneously, using the same strategy to train communities in other areas[267].

11.3.4 Quintana Libre

Quintana Libre is a community network developed by the NGO AlterMundi[268] and located in the area of José de la Quintana, in the Argentine province of Córdoba. Argentina is classified as a developing economy and in 2016 it ranks 55th on the

266 According to the Mexican Institute of Statistics and Geography, the GDP per capita of the state of Oaxaca in 2015 was US $ 3,615. See INEGI (2015).

267 See, for example, the SayCel cellular network project, available at <http://tinyurl.com/ycn3oksh>.

268 See <http://altermundi.net/>.

GlobalICTsDevelopment Index among the 174 members of ITU[269]. In this context, the goal of AlterMundi is to help small communities build their own communication infrastructure, thus overcoming the digital pits that affect rural areas. In particular, the purpose of the AlterMundi model[270] is to overcome the challenges imposed by the rural environment in which community networks are frequently established. Since its creation, AlterMundi has strived to design an efficient, economical and easily implementable and replicable technology, in order to overcome not only the reduced income[271] and the lack of infrastructure, but also the shortage of technical experts, who generally characterize rural areas.

The Quintana Libre network is structured in 70 nodes that provide Internet access for some 280 connected devices. Although it has been maintained through voluntary work, the AlterMundi association has obtained several financing to develop the community connectivity model and test it through the QuintanaLibre network. AlterMundi currently employs 15 people and several individuals have been hired to develop software, hardware and produce documentation, creating innumerable jobs since the creation of Quintana Libre in 2012. Quintana Libre was created in the context of a collaboration between AlterMundi and the National University of Córdoba with the objective of sharing infrastructure and promoting research and development in relation to community networks. The establishment of a 50 km link, which allows direct connection to the communications tower of the National University of Córdoba, connects QuintanaLibre with the rest of the Internet, allowing to exchange data freely.

This collaboration allows all the networks associated with AlterMundi to use the broadband of the University, when the university network is not used by students and academic staff during the night and on weekends, thus making the best use of a resource paid for by public funds.

---

269 See ITU (2016: 12).

270 For an analysis of the AlterMundi network model, see Belli, Echánz & Iribarren (2016).

271 According to the World Bank, Argentina's GDP per capita was equal to US $ 19,934, in 2016. However, the data relative to rural Argentina can be significantly lower. Consult <http://databank.worldbank.org/data/reports.aspx?source=2&series=NY.GDP.PCAP.PP.CD&country=>.

The members of QuintanaLibre have developed several applications adapted to the needs of the local community, including a local information portal, an instant messaging service, a VoIP server, a community radio transmission, a file sharing system and game applications. In addition, AlterMundi affiliated networks provide Internet access for three schools, which are connected through the regional network, as well as to public spaces such as plazas, bus stops and local cultural centers.

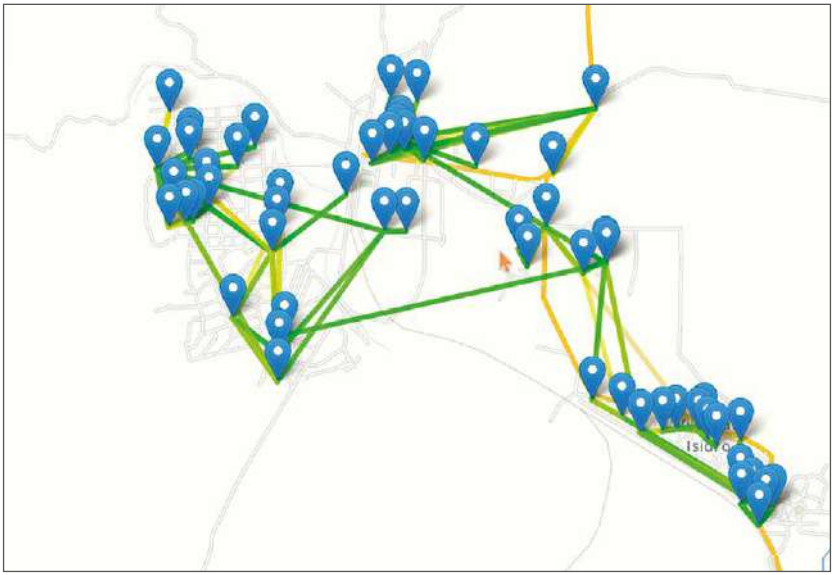


Figure 4: The distribution of the nodes of QuintanaLibre, in July 2016[272].

The main server of AlterMundi, hosted in the data center of the University of Córdoba, is used to facilitate the services of QuintanaLibre and provides different services to other community networks, both in Argentina and abroad.

These services were developed in association with the collective Code Sur[273], with the objective of providing infrastructure and development resources that promote the development and organization of local communities, promoting socialization among individuals. The partnership established in the context of the South

272 See <http://bit.ly/2tmsutX>.

273 Consult <https://www.codigosur.org/>.

Code has been particularly fruitful, leading to the development of a wide range of open source applications, including hosting, transmission and email services, as well as virtual private network (VPN) services[274].

11.4 Conclusions: challenges and opportunities of Community Networks

The examples discussed in the previous section demonstrate that community network initiatives can be successfully established in several contexts. These initiatives can be considered as an excellent example of concrete implementation of the self-determination of the network, empowering individuals with the possibility of reaping the benefits of connectivity and unleashing many positive external effects, capable of improving the quality of life of entire communities. The fact that community networks are participatory initiatives does not mean that individuals and organizations share their resources and coordinate their efforts to build network infrastructures. This also means that the individuals involved in the project, the implementation and the maintenance of the networks can learn and experience first-hand how Internet technology works. As such, local populations, previously excluded from the information society, have the possibility of developing the necessary capacities to benefit concretely from connectivity, through communication, acquisition of knowledge and, most importantly, the creation and exchange of innovative applications and electronic services adapted to meet the needs of the local community. Such initiatives have, therefore, the potential to lead to entirely new socio-economic ecosystems, built by local communities for local communities and, in addition, fundamentally *bottom-up*.

However, it is important to highlight that the projection, construction and management of a community network should be considered as tasks that need solid planning. The realization of sustainable and successful community networks requires the definition of a long-term strategy and a stable governance

274 Consult <https://www.codigosur.org/services>.

structure, capable of integrating local institutions as partners. It is thanks to the inclusion of these elements that the networks analyzed in this chapter were able to thrive under very different circumstances and, therefore, should be considered essential requirements for any community network. In particular, the cases analyzed showed that the sustainability of community networks brings an enormous benefit of cooperation with local institutions, such as public administrations, schools, universities, libraries or hospitals. Collaboration with existing institutions can reduce costs considerably, sharing costs and optimizing resources, and favor the stability and economic and organizational sustainability of the networks. In addition, this type of multistakeholder cooperation, involving public institutions, local civil society and local entrepreneurs, exemplifies in a significant way the positive externalities that only community networks have managed to generate so far, maximizing the positive benefits of connectivity, creating business opportunities and strengthening social relationships in local communities.

It is important to note that these last elements are precisely what differentiate community networks from other "traditional" strategies proposed so far to "connect the disconnected." In fact, unlike the strategies typically promoted by business actors, the objective of community networks is to allow the local population to autonomously determine how to connect, building new infrastructures and generating new services in a democratic and bottom-up manner. In this perspective, the infrastructure built by local populations should not be considered the "last mile" of the network, but the "first mile", which is developed and used autonomously by empowered communities, where individuals fully enjoy the right to network self-determination.

As Norberto Bobbio has often argued, rights emerge gradually, being the results of the "battles that human beings fight for their own emancipation and transformation of the living conditions that those struggles produce[275]." It is not absurd to argue that, just as individuals enjoy the fundamental right to freedom of expression

275 See Bobbio (1993: 26).

or to basic education, they should also be able to enjoy the right to network self-determination. There is no reason why individuals should not associate freely to democratically define the design, development and management of the network infrastructure as a common good, in order to seek to transmit and receive freely, information and innovations.

As shown in the examples analyzed in this article, the affirmation of a right to self-determination of the network is happening in fact, even before being consecrated de jure. The proliferation of community networks offers an obvious example of how members of communities from any context are willing and able to establish and organize a network infrastructure to improve their living conditions when they have the possibility to do so. In addition, the analyzed examples reveal that when groups of individuals with a strategic vision and a viable plan led the connectivity efforts, the result can be impressive, especially when connectivity is seen as a means of empowering people through education, new forms of community organization and new business opportunities. In this sense, network self-determination and the establishment of community networks should be facilitated and promoted by regulators to contribute positively to the elimination of existing digital gaps.

11.5 References

Antunes Caminati, F. Diniz R., Orlova A., Vicentin D., Olivier P.J. and Lara M., Beyond the last mile: Fonias Juruá Project – an HF digital radio network experiment in Amazon (Acre/Brazil) in Belli L. (Ed.) (2016b)

Baig *et al.* (2015). Guifi.net, a Crowdsourced Network Infrastructure Held in Common. In Computer Networks. N° 90. <http://dx.doi.org/10.1016/j.comnet.2015.07.009>.

Baig, R. *et al.* (2016). Making Community Networks economically sustainable, the guifi.net experience. GAIA '16 Proceedings of the 2016 workshop on Global Access to the Internet for All. <http://dl.acm.org/citation.cfm?doid=2940157.2940163>.

Belli, L. (2016a). De la gouvernance à la regulation de l'Internet. Berger-Levrault: Paris.

Belli, L. (Ed.) (2016b) Community Connectivity: Building the Internet from Scratch Annual Report of the UN IGF Dynamic Coalition on Community Connectivity. <http://tinyurl.com/comconnectivity>.

Belli, L. (Ed.) (2016c). Net Neutrality Reloaded: Zero Rating, Specialised Service, Ad Blocking and Traffic Management. Annual Report of the UN IGF Dynamic Coalition on Network Neutrality. Rio de Janeiro: FGV Direito Rio Edition. <http://tinyurl.com/zerorating>.

Belli L. (2017). "Net Neutrality, Zero rating and the Minitelisation of the Internet." Journal of Cyber Policy. Routledge. Vol. 2. N° 1. <http://dx.doi.org/10.1080/23738871.2016.1238954>.

Belli L. (Ed.) (2017b). Community networks: the Internet by the people, for the people. Official Outcome of the UN IGF Dynamic Coalition on Platform Responsibility. Rio de Janeiro. FGV Direito Rio. <http://bibliotecadigital.fgv.br/dspace/handle/10438/19401>.

Belli, L. (2017c). The scramble for data and the need for network self-determination. OpenDemocracy. <https://www.opendemocracy.net/luca-belli/scramble-for-data-and-need-for-network-self-determination>.

Belli L. and P. De Filippi, P. (Eds.) (2016.) Net Neutrality Compendium: Human Rights, Free Competition and the Future of the Internet. Springer. <http://www.ohchr.org/Documents/Issues/Expression/Telecommunications/LucaBelli.pdf>.

Belli L. Echániz N. and Iribarren G. (2016). Fostering Connectivity and Empowering People via Community Networks: the case of AlterMundi. In Belli L. (Ed.) 2016b.

Belli L. Schwartz M., Louzada L., (2017). Selling your Soul while Negotiating the Conditions: From Notice and Consent to Data Control by Design. In The Health and Technology Journal. Vol 5. N° 4. Springer-Nature. <https://link.springer.com/article/10.1007/s12553-017-0185-3>.

Beverungen A., Böhm S., Land C. (April 2015) Free Labour, Social Media, Management: Challenging Marxist Organization Studies. Organization Studies. Vol 36, Issue 4. <https://doi.org/10.1177/0170840614561568>.

Bobbio N. (1993). L'età dei diritti. Turin: Einaudi, 1993. Translated by Cameron A. (1996). The Age of Rights. Polity Press: Cambridge.

Chakravorti B. (16 February 2016). Lessons from Facebook's Fumble in India. Harvard Business Review. <https://hbr.org/2016/02/lessons-from-facebooks-fumble-in-india>.

Cristescu A. (1981). *The right to self-determination*: *historical and current development on the basis of United Nations instruments.* Study prepared by Aureliu Cristescu, Special Rapporteur of the Sub-Commission on Prevention of Discrimination and Protection of Minorities. Unied Nations. New York. <http://www.cetim.ch/legacy/en/documents/cristescu-rap-ang.pdf>.

Christl W. (June 2017). Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions. A Report by Cracked Labs, Vienna. <http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf>.

Echániz N. (2015). Community networks: Internet from the first mile. In FRIDA: 10 years contributing to development in Latin America and the Caribbean. <http://lacnic.net/frida/FRIDA-book2015-en.pdf>.

Fondo Monetario Internacional (IMF). (2017). World Economic Outlook Database. Washington, D.C.: Enero 16, 2017. <https://www.imf.org/external/pubs/ft/weo/2016/01/weodata/index.aspx>.

Foro Económico Mundial (WEF). (2011). Personal Data: The Emergence of a New Asset Class. <http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf>.

GSMA. (9 February 2016). Connecting the Unconnected: Unlocking Human Potential through the Power of the Mobile Internet. <https://www.gsma.com/newsroom/blog/connecting-the-unconnected-unlocking-human-potential-through-the-power-of-the-mobile-internet/>.

Greenleaf G. (2017). Global Tables of Data Privacy Laws and Bills (5th Ed 2017). 145 Privacy Laws & Business International Report. <https://ssrn.com/abstract=2992986>.

INEGI. (2015). Producto Interno Bruto Per Cápita por Entidad Federativa. <http://www.inegi.org.mx/est/contenidos/proyectos/cn/pibe/tabulados.aspx>.

ITU. (2016a). ICT Facts and Figures 2016. <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf>.

ITU. (2016b). Measuring the Information Society Report 2016. <http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-w4.pdf>.

ITU. (2017). Working together to achieve Connect 2020 Agenda Targets. A background paper to the special session of the Broadband Commission and the World Economic Forum at Davos Annual Meeting 2017. <http://broadbandcommission.org/Documents/ITU_discussion-paper_Davos2017.pdf>.

McDonald A.M. and Cranor L.F. (2008). The Cost of Reading Privacy Policies. In I/S: A Journal of Law and Policy for the Information Society. 2008 Privacy Year in Review issue

Kuneva M. (31 March 2009). Keynote Speech. Rundtable on Online Data Collection, Targeting and Profiling. Brusseks, European Commission. <http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm>.

Ostrom, E. (1990). Governing the commons: the evolution of institutions for collective action. Cambridge University Press. <http://wtf.tw/ref/ostrom_1990.pdf>.

Pun M. *et al*. (September 2006). Nepal Wireless Networking Project. Case Study and Evaluation Report. <http://lib.icimod.org/record/12552/files/4163.PDF>.

Rey-Moreno C. (May 2017). "Supporting the Creation and Scalability of Affordable Access Solutions: Understanding Community Networks in Africa". Internet Society.

Rey-Moreno C., Blignaut R., May J., and Tucker W. D. (2016). An in-depth study of the ICT ecosystem in a South African rural community: unveiling expenditure and communication patterns. *Information Technology for Development*, *22* (sup 1), 101–120. <http://doi.org/10.1080/02681102.2016.1155145>.

Saldana J. *et al*. (Eds.) (August 2016). Alternative Network Deployments: Taxonomy, Characterization, Technologies, and Architectures. Request for Comments: 7962. <https://www.rfc-editor.org/rfc/rfc7962.txt>.

Schuler D. (1996). New Community Networks: Wired for Change. ACM Press. <http://publicsphereproject.org/ncn/>.

Shearlaw M.(Monday 1 August 2016). Facebook lures Africa with free internet – but what is the hidden cost?. The Guardian. <https://www.theguardian.com/world/2016/aug/01/facebook-free-basics-internet-africa-mark-zuckerberg>.

The Economist. (6 May 2017). The world's most valuable resource is no longer oil, but data. <https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource>.

World Bank. (2016). Digital Dividends. World Development Report 2016. <http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf>.

WEF. (January 2011). Personal Data: The Emergence of a New Asset Class. <http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf>.

12 Building Community Infrastructure: Disruptive Technologies and Models

Christian O'Flaherty

Abstract

The article aims to demonstrate how the future of Internet and sustainable connectivity should rely on the principles of collaboration and cooperation to reach regions poorly served by commercial Internet service providers. In order to do this, this paper uses a number of already existing practical examples to briefly explain community networks, addressing their characteristics and the challenges they face in expanding this model. In addressing technical and regulatory barriers to the application of community networks, the article lists a number of obstacles, such as legislation, licenses and licenses related to spectrum management and the use of public infrastructure, and also indicates the need to develop adequate materials for networks alternatives, from the construction of equipment, through the development of standards and protocols and equipment training to operate this entire system. Finally, reiterating ISOC's motto, this work highlights the need for disruptive models of governance and sustainability for community networks – models that will be fundamental to achieving the goal of making the Internet for all.

12.1 Introduction – Internet Culture

Is it possible to extend the Internet model to the construction of Infrastructure?

In its origin, Internet was a series of experiments among universities that, although it greatly excited the researchers who worked on the project, none of them imagined the impact it would have on the entire world. This spirit of collaboration and fraternity defined the process used to agree on how things should work in regards to the Internet.

The evolution of these community processes ended up shaping what we now call the Internet ecosystem and the collaborative

Internet model. This culture, forged at the beginning, gave rise to organizations that are currently fundamental in the development of the Internet, such as the *Internet Engineering Task Force* (IETF), where the standards are agreed upon, or the regional Internet registries, which manage the numerical resources.

This model was organized and formalized when the IETF began to document what those open (inclusive) and transparent processes should be like. The foundations were laid for the organizations that manage resources on the Internet to do so in a fair, transparent and efficient manner, trying to avoid the negative effects that can be produced by companies, governments or any person or organized group that wants to "control" those resources. That collaboration between all the interested parties (which we call *multistakeholder* model)[276] is the heart of Internet governance. This cooperation and collaboration extends to almost all the areas that the Internet touches and has allowed an unprecedented global expansion.

In the creation of infrastructure, the closest to that collaborative culture imposed by the pioneers of the Internet are the community networks that, for now, are experiments; but that could be the only sustainable model to connect areas not served by commercial providers.

12.2 What are community networks?

A model that has worked very well when the Internet does not reach remote places, is for the community to build the network to reach the Internet (not waiting for a provider to reach their community but instead building the network to reach the nearest provider). That implies several challenges[277] and requires technological, legislative changes, new standards and communities that are capable of building and operating community infrastructure[278].

Community networks have unique characteristics that require evolution and disruptive changes in both technologies and in the management of resources (use of public infrastructure, spectrum

276 See ISOC (2016).

277 See Belli (2015).

278 See ISOC (2017).

management, Internet resources, etc.). There are many examples in the world and different models that have shown that it is possible to connect areas where the market or commercial Internet cannot justify the necessary investments[279].

We are in a transition stage. The experiences prove that there are many models that make these community networks sustainable and effective. Now we must begin to formalize and generalize these models to achieve the necessary scale and impact. We must promote changes in regulations and technologies, in governments and companies, in equipment manufacturers and in *open-source* software. It will be necessary to organize and train communities, involve NGOs so that they have the capacity and resources to help them, convince companies that this does not affect their business and be sensitive to the needs and differences of the people we are connecting.

12.3 25 Years of Internet Society

More than twenty-five years ago (in 1992), the Internet Society was created and the first important steps in the governance of the Internet that we currently enjoy took place. In those same years, the Internet ceased to be an Academic network where costs were shared among all members of the network, in order to give rise to companies that could do business reselling that traffic to end users or other companies.

It is known that this commercial use of the Internet accelerated its growth and transformed telecommunications throughout the world. These changes, in turn, impacted on the commercialization of products, in business, in education, generating progress and improvement in the societies that almost all of us enjoy and that we still do not fully perceive and take advantage of. The billions of people who connect every day to the Internet can enjoy a service that improves their lives, but unfortunately generates more and more difference with those who still cannot be connected[280].

279 See Belli (2017).

280 (World Bank, 2016).

The Internet owes its great success to the companies that built the infrastructure that we currently use. However, it will be difficult for these companies to justify the necessary investments to reach the billions of people that are missing to be connected. Additionally, it would not be good for other companies to justify those investments at the expense of personal data, information or any other resource that new users can contribute without knowing it.

Many of the disconnected communities are in places of very difficult access, or are places with few inhabitants, or incomes that do not allow the payment of an Internet access fee without compromising their own support. In order to continue growing and connecting the most difficult places, we will need a different model that can complement the commercial one. We cannot expect companies to lose money by investing in areas where they will not profit. It will not work to demand or subsidize connections in those places because it will not be sustainable and it will not scale[281]. Nor would it be good if the new user´s online experience is different from what we have known so far, condemning them to limited Internet access, or being conditioned to the capture of their personal information, or mortgaging their future resources or compromising their privacy

At the Internet Society we are interested in promoting community initiatives in these unprofitable places. We think of it as a return to the academic origins of the Internet, where everyone makes the effort to "get" to the Internet instead of waiting for the Internet to reach us. It is extending to the construction of infrastructure the concept of cooperative and collaborative model that we use for the administration of other resources (such as domain names or IP addresses). For the model to be sustainable, those who build and operate that network must agree on its "governance model" just as we have done in other areas of the Internet.

12.4 Disruptive technologies and regulations

Other necessary changes are the technological and the regulatory ones. In order for these community projects to flourish, it will be

281 Cáceres (2011:15).

necessary to update our rules (legislation, permits, licenses, etc.) so that those places that are not commercially viable are free to use resources that are normally reserved for companies that pay the corresponding licenses. A clear example is the use of frequencies for cellular networks or point-to-point links. In the current Internet, to be able to take advantage of the spectrum efficiently, it is necessary to maintain an order that avoids interference between operators. This orderly use of the spectrum is currently achieved with the payment of licenses. These licenses, depending on the frequency band, the amount of spectrum, and possible businesses, can cost millions of dollars. This model that, in principle, seems to harm companies, actually favors those already established because it hinders the entry of new suppliers. Although the model has worked successfully throughout the world, it should only be applied in areas where there is commercial interest. It is not reasonable to keep the same model in places not connected due to lack of customers, because the spectrum is idle and the people unconnected. What is pending update, is the possibility of using those frequencies when no commercial operator wants to invest in those places[282]. The same can happen with rights of way, use of poles, towers, public spaces, etc.

Another example of disruptive change in wireless technologies is the use of unused TV frequencies (also called *TV White Spaces* because some of those free spaces were left between analog TV channels). Now the term *TV White Space* (TVWS) is being applied more generally to technologies that allow radios to be used without causing interference to functioning services (and below 1Ghz). In countries such as Colombia, the necessary regulatory changes have been made to take advantage of this and there are community network projects implemented with radios that use these frequencies[283].

In order to make a more efficient use of the spectrum not only regulatory changes are needed. Standards will also be needed to allow manufacturers to develop low-cost equipment that takes advantage of the possibilities that will enable these regulatory

282 ISOC (2017).

283 Makaia (2017).

changes. Following the example of TVWS, there is a protocol documented by the IETF for access to the database needed to avoid interference (PAWS: *Protocol to Access White-Space Databases*[284] [285]). For these technologies to begin to spread, it will be necessary to have software for these databases (preferably *open-source*) and equipment that implements those protocols. These new technologies will be used in areas without connectivity (and usually without television). Since these places do not have commercial appeal, we cannot expect the industry to promote those regulatory changes, develop those new standards or implement the necessary software. It is the Internet community that must organize to take advantage of and spread these disruptive technologies.

12.5 The equipment must also evolve

A similar evolution is required by the equipment that is currently used for the Internet. The evolution of the current model has favored technologies and standards needed by the industry and the Internet (or commercial Internet) business. That evolution followed the Internet model, defining the technologies and open standards that were needed to build the networks we use today. The existence of these standards allows manufacturers to build equipment that will work in networks of different commercial providers and "extend the network" to their customers. With these standards and large production volumes, the industry has managed to reduce costs to build access networks, high capacity links and cover large distances, allowing the connection of more than 3 billion people.

In some cases, the unconnected communities are organized and can take advantage of these technologies and build access networks or low cost links to reach the areas already connected. Some of these standards (such as Wi-Fi, or technologies for access networks using Fiber Optics [PON] or equipment for mobile networks, *open-source*) have been used successfully in community networks[286]. There are examples where the people of the community

284 See Mancuso, Probasco and Patil (2013).

285 See Chen *et al.* (2015).

286 Guifinet is an example of multiple Community Networks based on existing technologies: <https://guifi.net/maps>.

are organized to create, among all, the necessary infrastructure to provide these services, for thousands of households and in some cases also companies (for example, gui-fi.net in Catalonia[287]) where conventional equipment is used and the infrastructure is created by the community.

In other cases, the commercial equipment does not serve to meet the needs of these alternative networks. Many community networks must replace the firmware installed with ad-hoc versions that implement the protocols and services they need. The software used for these networks is *open source* and generally developed by members of the same community networks. This disruptive change in the development of software for Internet infrastructure is not only seen in community networks but in many other new technologies that are being implemented on a large scale (SDN, NFV, etc[288].) which also take advantage of the agility and capacity of the *open source* community to get better products and services in less time and at a better cost.

12.6 Why new technologies for the equipping of community networks?

To use the Internet, we are currently connected by a company that is responsible for the service within its network and that pays another company to connect with the rest of the Internet. The equipment, protocols, networks and software used are designed for this model.

In the non-commercial or community built infrastructure, our equipment can be used to reach other unconnected areas, and thus the network is extended.

They grow by connecting with each other and sharing infrastructure and costs. This efficient model of resource use, allows to reach distant places without large investments since each one only deals with connecting the nearest neighbor and shares the additional expenses. This is how the Internet worked until the 1990s when the model evolved into a commercial model and achieved a global

287 See <https://guifi.net/>.

288 See <https://www.openstack.org/>.

scale. Now, we have the opportunity to recover the collaborative spirit that the Internet had in the beginning to complement the commercial model and reach the unconnected.

Due to the lack of interest of the industry, some of the technologies needed to use this collaborative model are not standardized or are the property of the companies. For example, the available Wi-Fi equipment does not allow the creation of mesh networks[289] because there are no standardized routing protocols. In a mesh Wi-Fi network, a new home can connect to the neighbor's Wi-Fi to reach the Internet and will be available so that another neighbor can connect with it. In that case, the equipment that we install at home should implement a routing protocol that interacts with the neighbor's equipment. In addition, the hardware and software must be designed so that the equipment allows the re-use of resources in a scalable way, avoiding for example that the farthest points have bad service when the "closest" consume the entire BW.

There are also not enough management tools for a shared network to allow quick diagnostics or detection of network abuse and problems. In a network with these characteristics, management is much more complicated compared to a commercial network that is managed by a single operations team. The management of a shared network requires the active collaboration of all those connected since a problem in one of its nodes (for example, a house) can affect the service of all the other nodes (houses) that are connected to it.

Another example is the access service using cell phones. Currently the hardware needed to build these networks is more accessible (compared to the millionaire investments that companies had to make years ago). Technology has evolved so that mobile networks are efficient for Internet traffic because it is what users use.

That evolution generated a disruptive change in the cellular industry, making the current mobile business and technologies closer to the Internet model than to the traditional telephony model as it was until now. While we can take advantage of some

289 See <https://en.wikipedia.org/wiki/Wireless_mesh_network>.

changes, equipment, standards and software still need to evolve. For community cellular networks, the open-source software available only allows 2G service deployment (we expect stable implementations of *Long Term Evolution* (LTE) for 2018). If the service continues to evolve as it has done so far, we will have equipment, software and regulations that will allow the deployment of community networks for low cost, easy-to-operate cellular service. There are cases in Mexico where community networks offer sustainable GSM service[290].

12.7 Disruptive models for governance and sustainability – Internet is for Everyone

The slogan of the Internet Society is "Internet is for Everyone" and in the case of the community network this is a fact. If we think of the community network as a common good (which is owned by all), clear rules are needed, agreed and respected by all participants to avoid the "tragedy of the commons".

The challenge is to get everything agreed by the community that uses the service. These include management of the network, the distribution of costs, the expansion and deployment of new infrastructure, the *upgrades*, repairs and equipment changes, the implementation of new services, etc., which must be coordinated to avoid project failure. We call this process of decision making governance of the network, and the necessary changes are as innovative as the technological ones.

There are many community networks and there are more differences in their governance models than similarities. We can only think of common principles and reference models that will be adapted case by case in order to support the projects that are initiated. Organizations, governments and companies that wish to support these projects will need to trust the communities and assume some kind of commitment if they wish to take advantage of these resources, such as permits, rights of use, financing or equipment donation.

290 See <https://www.rhizomatica.org/resources/>.

Is it possible to have transparent principles and processes so that the funds contributed by organizations and governments can be used efficiently to build community infrastructure? Can these new networks belong to everyone's Internet trust?

12.8 Conclusion

At the Internet Society, we trust that the model that enabled Internet growth until now will evolve to facilitate the construction of community infrastructure. The necessary changes in each of the areas are already being discussed. There are large community projects that demonstrate its viability and the great potential to reach the places that are currently disconnected. We invite all interested parties to collaborate with the Internet Society so that The Internet is for everyone.

12.9 References

Banco Mundial (World Bank) (2016). World Development Report 2016: Digital Dividends. Washington, DC: World Bank. doi:10.1596/978-1-4648-0671-1.

Belli, L. (Ed.) (2017) Community networks: the Internet by the people, for the people. Official Outcome of the UN IGF Dynamic Coalition on Community Connectivity. Rio de Janeiro. FGV Direito Rio.

Belli, L. (Ed.) (2016) Community Connectivity: Building the Internet from Scratch Annual Report of the UN IGF Dynamic Coalition on Community Connectivity. <http://tinyurl.com/comconnectivity>.

Cáceres, R. B. (2011). Uso de los fondos de acceso universal de telecomunicaciones en países de América Latina y el Caribe. <https://repositorio.cepal.org/bitstream/handle/11362/3912/S2011088.pdf>.

Chen, V., Ed., Das, S., Zhu, L., Malyar, J. y P. McCann (2015). Protocol to Access White-Space (PAWS) Databases. Request for Comments: 7545. <https://www.rfc-editor.org/info/rfc7545>.

Internet Society (2016). Internet Governance – Why the Multistakeholder Approach Works. <https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/>.

Internet Society (2017). Policy Brief: Spectrum Approaches for Community Networks. <https://www.internetsociety.org/policybriefs/spectrum/>.

Mancuso, A., Probasco, S. y Patil B. (2013). Protocol to Access White-Space (PAWS) Databases: Use Cases and Requirements. Request for Comments: 6953. <https://tools.ietf.org/html/rfc6953>.

13 Re-think Public Policies to Close the Digital Divide in Latin America

Pablo Bello and *Andrés Sastre*

Abstract

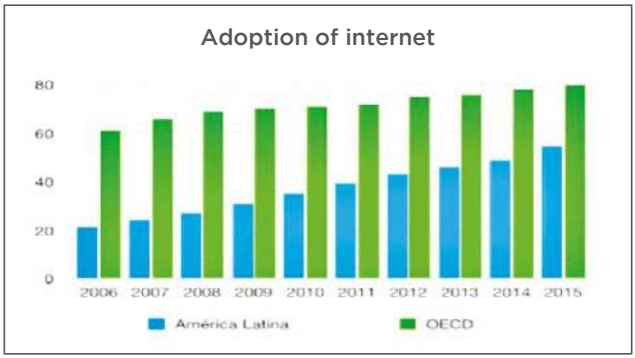
Latin America has made significant progress in recent years in terms of connectivity, but there are still significant challenges to achieve the closing of the digital divide and the full insertion of the region in the Information Society. Understanding the transformations that have taken place in the digital ecosystem in recent years, in particular the phenomenon of convergence, and the factors that influence the decision-making processes regarding investments in networks is fundamental for public policies to promote the configuration of virtuous circles of competition, innovation and greater coverage of connectivity services. Recognizing the notable advances of recent years allows us to assess those factors that have helped to democratize access, but at the same time it highlights the magnitude of the pending task and confirms that the path that remains to be traveled is more complicated than the already traveled. For Latin America to resume rhythms of economic growth that reduce poverty and generate opportunities for progress and equality, it is essential to increase productivity and transform the structure of value creation. That is why the digitalization of production processes is one of the most important economic policies that we have to carry out. Achieving the closing of the digital divide and having a world-class connectivity infrastructure is a necessary, though not sufficient, condition for moving in that direction.

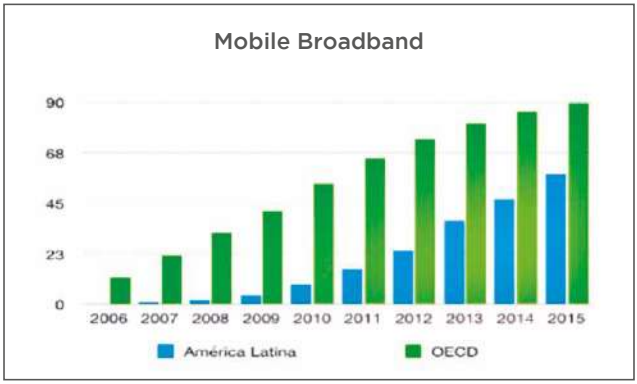
13.1 Introduction

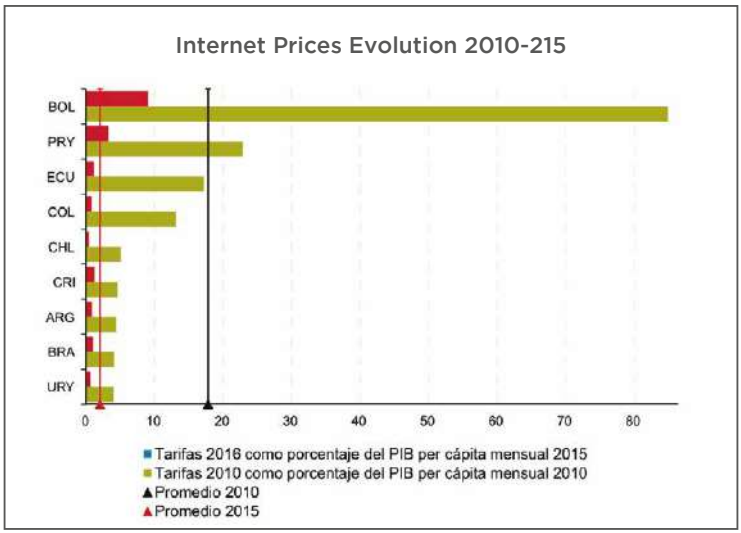
Latin America has taken significant steps in recent years in favor of closing the digital divide. People, Households and businesses are increasingly connected, the speeds – as a quality indicator – have increased steadily, and prices in real terms have fallen.

Although there are still significant gaps between urban and rural areas, high-income sectors and the poorest, and large companies and micro-enterprises, among others, progressively the region is closing the gap with the most advanced countries in the region in terms of Internet access. This is fundamentally the consequence of the rapid development of telecommunications networks in recent years, in an environment of openness to investment and competition, which has allowed democratizing access to telephony and is favoring digital inclusion. Public policies have played a central role in this history of advances, boosting competition, laying the foundations for private investment, and especially, designing instruments to expand the supply of services to less profitable areas for companies. The telecommunications infrastructure of Latin America is, by far, the most robust and widespread infrastructure in the region.

Graphs 1, 2 and 3. Adoption of Internet, Mobile Broadband and Prices.





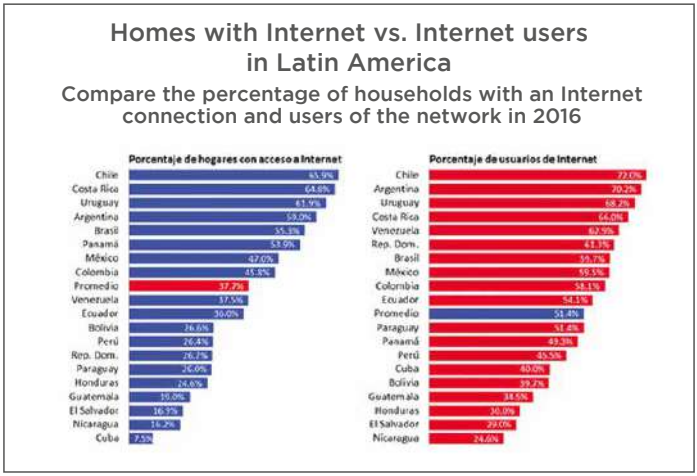


Source: CEPAL

However, despite the undeniable advances, the region still faces significant challenges. Nearly half of Latin Americans still do not use the internet; the access speeds are substantially lower than those of the developed countries; there remains a strong inequality in access between countries, within countries between rich and poor households, and between inhabitants of cities and rural areas. Latin America is the most unequal region in the world. In the information age, unequal access to knowledge and the tools offered by the Internet deepens inequalities, while at the same time sharpening the structural fragmentations that conspire against economic growth and social progress[291]. For both ethical and economic reasons, it is essential to close the digital divide and achieve a world-class connectivity infrastructure that supports the productive transformations that the region demands. This is a necessary condition, but not sufficient, to advance development.

291 (World Bank, 2016).

Graphic 4. Households and Internet Users in Latin America.



Source: Mediatelecom

This article offers a reflection on the factors that explain the advances achieved in recent years and, from there, proposes a pragmatic and realistic vision to achieve the accelerated closing of the digital divide. In order to design good public policies, it is necessary to correctly assess progress and challenges, recognize successes and mistakes. Although the "movie" of Latin America is going in the right direction, the "photo" to this day is still not satisfactory. The reality is that we are halfway (half full glass, half empty glass), and in the ideal position to see the successes and errors to date and set new goals.

13.2 The transformations of the digital ecosystem

Connectivity in Latin America has advanced significantly in the last 20 years. Internet usage rates in the region are close to 55%, not so distant from the more advanced countries that are close to 70%. The digital divide continues to be centered in rural areas and especially in the social sectors with fewer resources, the base of the social pyramid. **The digital divide is above all the poverty gap**. Achieving the full incorporation of lower income families into the Information Society is Latin America's greatest

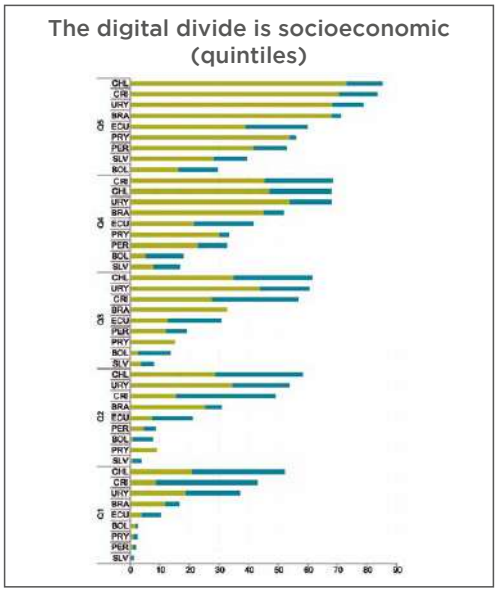
challenge in closing the digital divide. This without neglecting that as the connectivity progresses the traffic continues to grow and we must adapt the infrastructure to that demand. This means the need to continue investing in new quality networks, such as fiber optics and 4G, and new challenges such as 5G and *Internet of Things* (IoT).

In order for Latin America to close the digital divide and have a first-class connectivity infrastructure, an investment of the order of USD 400 billion accumulated in 7 years is necessary, according to a study by cet.la (2014). This in a context in which the income generated on average per user to remunerate the networks (*Average Revenue Per User* u ARPU) have been systematically lowering[292] while regulations have increased costs, both those associated with the deployment of networks and operational ones, while at the same time they have tended to limit commercial flexibility.

The above also occurs within the framework of an accelerated process of technological transformation, that of convergence, which is redefining the economic foundations of the traditional telecommunications and digital services industry. Since the emergence of the competition of electronic communication services on different platforms (copper, fiber, mobile, satellite, etc.) and the packaging, until the explosion of the market of contents and services on the Internet, what is happening is a disruptive process that is modifying the model of remuneration and sustainability of the Infrastructure. This model assumed the return of investments mainly through payment for the consumption of services of various kinds, which could only be offered over physical networks. We are currently facing a more complex dynamic, in which there is a service (that of Internet access) that allows third parties to offer services and contents that compete with traditional ones, which do not contribute to financing connectivity infrastructures.

292 Mobile ARPU in Latin America is less than 10 USD per month, much lower than 31 USD in Europe or 49 USD in the United States.

Graph 5. Digital divide by population quintile.



Source: CEPAL

Thus, the intrinsic identity between network and service has been broken, producing a logical (virtual) disaggregation that allows substitutability in the supply of final services. In other words, consumers today can satisfy their communication and entertainment needs through services provided directly "over"[293] the access networks (that remunerate these networks) or through services provided via the Internet (which do not, or at least not completely), which naturally has implications for the economic sustainability of the model and implies a paradigm shift that moves us to rethink to rethink the regulation and public policies. This is expressed in the fact that the indicators that account for the profitability of investments in connectivity have deteriorated, despite the expansion in demand, which means that investing in Internet access is less attractive than in the past.

293 PoreheartedheartedOverThe *Top*(OTTs).For further information see the documents submitted to the consultation recently organized by the International Telecommunication Union: <https://www.itu.int/en/council/cwg-internet/Pages/consultation-june2017.aspx>.

Obviously, it is not a matter of establishing restrictions or regulations that hinder the offer of services over the Internet, nor a kind of confrontation between telecommunications companies and the Internet. The value of the digital ecosystem lies precisely in these services and in their virtuous relationship with the networks that allow their provision and access. The point is to understand that we are in a new paradigmatic scenario, characterized by greater competition in final services, which forces us to revise the very foundations of traditional regulation, understanding that the fundamental objective is the one we described at the beginning: close the digital divide and have a world-class connectivity infrastructure. An important part of the problems that are currently evident in the regulations come from the fact that only the telecommunications sector is still being considered and not the whole digital ecosystem. Most of them still obviate the existence of other players and elements of the value chain, such as services provided over the Internet or the so-called collaborative economy. This produces strong regulatory and fiscal asymmetries, as well as regulatory gaps that can be addressed, in particular due to the growing importance of data economy and two-sided markets. A regulation designed for the era of convergence has to strictly follow the principle of "technological neutrality"[294] and try to be limited to solving market or public interest problems.

Having this principle clear, the existing markets in the digital ecosystem should be understood by the services offered and the degree of substitutability of them, not by the technological form in which the services are provided. Hence the concept of Technological Neutrality, understood as the regulatory (and fiscal) treatment of services, regardless of the technology through which they are provided. An adequate regulatory approach based on technological neutrality would allow the consumer's choice to be made strictly by the attributes of the options and not by arbitrary differentials of regulatory or tax burdens, which would result in greater efficiency and social welfare, at the same time that it would

294 The **Technological Neutrality** is commonly defined as "the freedom of individuals and organizations to choose the most appropriate technology appropriate to their needs and requirements for development, acquisition, use or commercialization, without knowledge dependencies involved such as information or data."

avoid the distortions that conspire against the network investment remuneration model. The crucial element, consequently, is that under the paradigm of convergence, all operators must be able to offer without distinction all the services that technology allows, develop all business models that benefit society, and determine which is the necessary regulation for electronic communication and audiovisual entertainment services in the Internet age, regardless of whether said services are provided directly over a copper network, a mobile network or over the Internet.

13.3 Public policies

An adequate regulation for the context of current convergence is one that does not establish asymmetries between actors but on the contrary encourages a competitive and sustainable environment, which is flexible and oriented to solve market problems, and promotes trust through a correct institutional design, with clear rules and transparency. Including new actors does not necessarily mean regulating them, but, contrarily, rethinking the regulation of traditional services.

An important aspect that derives from the previous reflection has to do with data economy and two-sided markets. We do not intend here to make an approach in favor of the deregulation of personal data and privacy. On the contrary, we understand that a key aspect to achieve the accelerated development of the digital ecosystem necessarily involves building an environment of trust on the part of individuals and companies. As reported by the public opinion study conducted by IPSOS for CIGI[295], in Latin America the levels of digital trust are among the lowest in the world, which imposes the need to address the construction of adequate protection mechanisms. What is important is, once again, that the regulation be neutral, that is, it allows developing the same business models to all the actors, in order to avoid unfair competition that affects, in particular, those who must deploy the networks, and that the data economy benefits the whole society.

295 See CIGI-Ipsos (2017).

While we do not address the new realities already raised, and public policies remain focused on the logic of services designed for the pre-convergent era, investment will slow down, including the development of new models such as the IoT, and affecting the quality of the service and competition.

Estimates of the investment effort necessary to close the digital divide and have a world-class infrastructure may differ. We said earlier that, according to the calculations presented in the study published by the cet.la in 2014, it is required the order of 400 billion dollars of investment to match the indicators of service offer in Latin America with those of the OECD countries. But the supply of services does not guarantee demand, especially considering the budget constraint faced by many families. The central question we must ask ourselves is how to combine the strengthening and expansion of the market with the objective of maximizing the investment of companies and transferring efficiency gains and technological advances to consumers through competition, and at the same time to design instruments that allow achieving full inclusion and digital equity.

The experience of the last 20 years shows us the central importance of the telecommunications market to achieve accelerated progress in terms of inclusion. But it also teaches us that the market is not enough. Public policies that favor the expansion and depth of the market are required, and complement it to achieve the objectives that society demands. However, this is easier said than done. The problem arises many times because the objectives that society demands are not unique but are multiple and complex, often entering into contradiction, or at least in tension. Hence the relevance of deliberative processes based on evidence and the specification of objectives, good practices and a healthy democratic debate. But contradictions also arise when one loses sight of the logical meaning of the leverage of the state and the market based on the previously defined complementarity. Neither the market nor the state are ends in themselves. They are instruments of different nature that fulfill specific roles for the achievement of social objectives. That is why we emphasize democratic mechanisms to define and agree on these objectives, and from there on to apply the best institutional instruments of public policy to achieve them.

13.4 Challenges and political priorities

The challenge faced by public policies to close the digital divide is extremely complex and contradictory.

On the one hand, more investments in networks are required, both for coverage, capacity and quality, but at the same time it is expected that the prices for services will decrease, that the contribution of operators to the financing of the state will be increasing (spectrum, taxes), while the cost of deploying new networks increases (often by regulations and local governments) while increasing regulatory restrictions that limit the possibility of developing business models that generate additional income. Undoubtedly, it is an unsolvable equation.

A common error when discussing public policies is to confuse the objectives with the instruments. Another recurring error is that there is a tendency to underestimate the real restrictions (for example, the low level of ARPU in Latin America) and it is assumed that what is achieved (or not achieved) has more to do with wills than with the realities of each environment. Obviously, reality is more complex than desires. Politics demand the need to prioritize, to define which objectives are more important than others, to seek balance ("*trade-off*") that maximize social welfare, and find the most appropriate mechanisms to achieve it. Not all objectives can be achieved simultaneously. The essence of a political system lies in the institutional mechanisms to find those balances, which are not "better" or "worse", but rather express the preferences of society, especially in the case of democratic societies.

Obviously, the priorities of each country are different depending on their particular realities, their starting point, and the objectives that are defined. Therefore, we should never tend to make a "copy and paste" of the public policy agendas of other countries, in particular of developed countries. A problem of democratic quality and the adequacy of public policies derives from situations in which priorities are defined by those who have more voice instead of those who need it most (for example, if regulations are defined according to the needs of those connected and not by those of those not connected). In the countries of Latin America, as a result of the transformations of

the years of economic growth, social mobility and poverty reduction, we are experiencing the phenomenon known as "the middle income trap", characterized by emerging segments that demand regulations and policies that favor them (as is logical), but indirectly hurt the most vulnerable sectors, disadvantaged or lagged, while reducing growth rates slow down the mobility process. The transition of priorities from mass to quality, from minimum to recommended standards, of bandwidth coverage, imposes costs that make it more difficult to incorporate those who are left behind to the dynamics of modernity. This, which is inherent to progress, requires the design of specific public policies to avoid deepening inequalities.

That is why we place so much emphasis on the definition of priorities and on the role of politics. For example, the burial of cables constitutes a reasonable and desirable demand of the inhabitants of the neighborhoods with service coverage, but their cost can harm the expansion of the networks towards non-covered sectors. Greater regulation of the quality of services may favor those who are currently users, but at the same time it may make it more difficult to close the digital divide if this increases costs (and eventually prices), reducing margins and therefore incentives for investment in networks given the low ARPU previously mentioned[296]. The same can be said about strict regulations that prevent traffic management or different access marketing models. It is therefore essential to evaluate the costs and benefits of public policies based on democratically defined priorities.

The type of intervention carried out in a market can have effects of different nature that must be analyzed to understand the costs (direct, indirect, opportunity) that can occur. The Regulatory Impact Analysis (*Regulatory Impact Assessment* or RIA) is a valuable instrument for these purposes. In particular, we must bear in mind that what we are trying to achieve is the construction of a virtuous circle of investment and competition that favors inclusion and the harmonious development of the digital ecosystem.

296 It would be more interesting in this line, to explore ways of self-regulation of the industry in the quality criteria that do not increase the associated costs, where in a competitive environment the users are those who can reward or not the quality of the services, determining with your choice one company or another. Otherwise, excessive regulation of quality may lead to higher costs and the transfer of these costs to customers, with lower purchasing power being the most affected.

If we understand that the closing of the digital divide and the availability of world-class connectivity infrastructure are priority objectives of public policy, there is no doubt that investment should be at the center of concerns. The achievement of these objectives is only viable if networks and services are deployed through different technological solutions throughout the territories. However, increasing investment in telecommunications networks has seldom been one of the priority axes of public policies.

13.5 The importance of investment and competition

Investment in telecommunications is fundamentally a springboard for companies, most of them privately owned. Investment decisions respond, as is natural in any market, to the existence of an adequate expected return, which is determined by risk, by demand projections and the willingness to pay. It must be in the public interest that the telecommunications industry is a healthy, competitive and sustainable market. It is therefore fundamental that policy makers understand the investment decision process properly and favor conditions that stimulate them. It is not, in any case, to state that the policy should be for the benefit of private interest, but on the contrary, that for the market to maximize the social benefit it is necessary to generate the conditions for its expansion. It is not, either, to confuse market with companies, to favor the development of the market is not synonymous with protecting certain companies or avoiding competition. What we are talking about is how public policy generates the conditions to accelerate the development of the market, because that is the most efficient and effective way to achieve the closing of the digital divide and have the best connectivity infrastructure.

In Latin America, the conditions for the development of the telecommunications market are heterogeneous among the countries (see the following figure) and with multiple contradictions that are derived from many times the absence of a clear prioritization of objectives and other times for not understanding the previous reflection.

To put it in concrete terms, if you want to achieve lower prices for telecommunications services in a sustainable way and

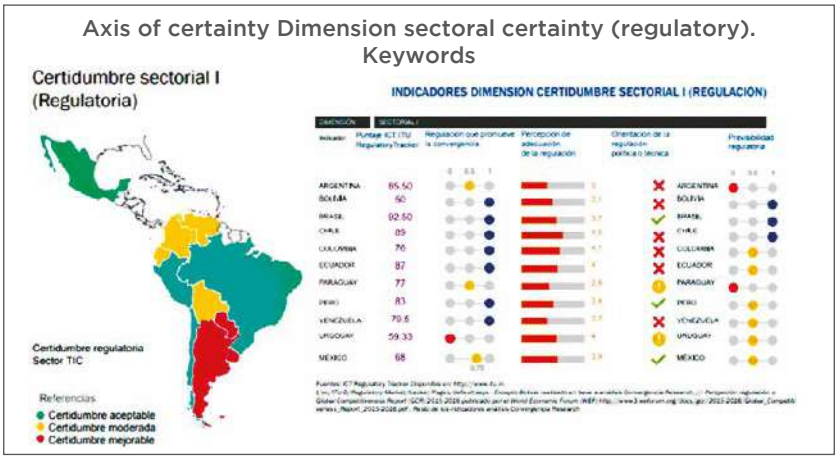
that maintains investment incentives, there is no doubt that competition among suppliers is required, but it also matters that the evaluation horizon of investment projects is as large as possible, that the associated risks to the development of these are the least since it impacts the profitability necessary for the project to be viable, the costs of deploying the networks are adequate, both in terms of money and time and procedures, that the structure of tax charges is fair, that the essential inputs to provide the services – for example, the radio spectrum- are allocated according to the objective of stimulating investments and not for collection purposes. In other words, to achieve more investments and lower prices, a necessary condition for closing the digital divide, it is essential to generate the conditions to reduce risks and uncertainty and reduce costs.

Many times policy makers, guided by laudable objectives, carry out interventions in markets that end up generating the opposite effects to those expected. And they have to do precisely with an inadequate understanding of the investor decision process. It is thought that mandatory sharing, unbundling of networks or the obligation to provide facilities to competitive operators (virtual for example, or even community networks) helps to reduce costs and promote digital inclusion. Sometimes it can be like that, but it can also have the opposite effect[297]. It is not a question of discarding heterodox solutions dogmatically in order to solve the challenge of closing the digital divide, but to avoid "displacement effects" that affect the aggregate investment. If these regulations increase risk, reduce profitability, or increase the cost of providing services or deploying networks, the final effect may even be worse than the initial situation, that is, they deepen it instead of helping to solve the problem. The fine art of regulatory policy involves finding the right balance to maximize social welfare, and this may involve network sharing, resale, disaggregation or social entrepreneurship

297 In particular, community networks can be an interesting solution to offer services in areas where there is no interest from companies, however, it is often not evident that these are really unattended areas ("gray areas"), especially in low-income urban sectors. If these solutions enter into competition with consolidated operators, situations that tend to discourage investment by them may occur. The above can be more complex if there is allocation of spectrum for this type of networks or regulatory requirements are raised to favor this type of networks (media sharing, spectrum, roaming, interconnection, wholesale regime etc) that create distortions in the market that affect the investment. It is not, again, to be "for" or "against" community networks, but rather how creative tools are designed to leverage and complement the market, avoiding substitution effects.

models such as community networks as long as they constitute co-adherents to the expansion of the market as an option of the investor and not as a mandatory burden. Generating the conditions and incentives to stimulate this type of model is positive, imposing them is often counterproductive. It is about guiding the market forces to generate the dynamics that maximize the social interest, for which the heterodox models must be leveraged in the market and complement it, not replace it.

Graph 6: Regulatory certainty in Latin America.



Source: Convergencia Research

But encouraging maximum market expansion is not enough. In the most remote sectors of the rural area the costs associated with the deployment of networks may be greater than the availability of the inhabitants to pay. There, public intervention is required, making use of various instruments to complement the role of the market.

Universal service mechanisms associated with public funds to subsidize supply or demand are central aspects of the gap closure strategy. However, international evidence shows contradictory results of the various intervention models[298]. It is naturally easier to address the problem of areas lacking coverage, as through incentives derived from spectrum allocation mechanisms (*beauty contest*) or competitive subsidies to the offer it is possible to close gaps.

298 Cáceres (2011).

However, the analysis of social profitability is critical to ensure that decisions implemented outside the market are efficient and effective.

Unfortunately, many times the investment projects decided by the State in Latin America have not fulfilled the social objective of effectively contributing to closing the digital divide by overestimating the expected demand, favoring specific non-priority social interests, or underestimating operational costs. Similarly, the budgetary restrictions of the States tend to limit the scope of these initiatives, even when they are well designed.

In the case of low-income urban areas, instruments of this nature are also required, which are all the more effective if they are leveraged in regulatory initiatives that encourage private investment and reduce the costs of providing services. Demand subsidies or tax exemptions can be adequate instruments, as long as there are good socio-economic targeting instruments, which regrettably does not happen in Latin America. Initiatives aimed at facilitating the use of goods for public use and state establishments in rural or low-income areas for the deployment of corporate connectivity networks while relaxing certain technical quality regulations can be effective, contribute to making certain private projects viable, and reduce the need for state contributions.

On the contrary, there may be public investment initiatives or projects carried out under public intervention schemes that may generate what in economics is called “displacement effect”, and which result in the substitution of one investment for another with very limited net effects.

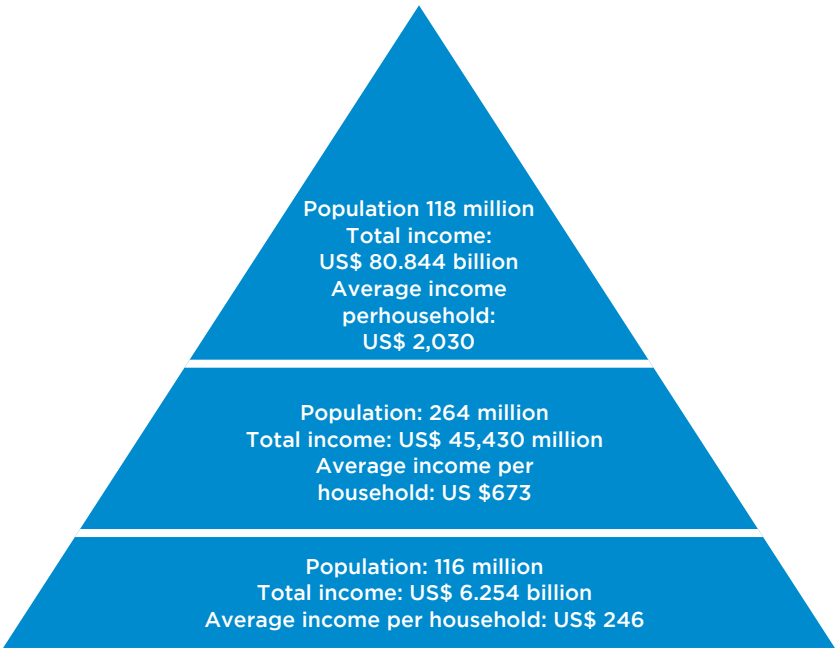
The point is, as we have been pointing out, that it is very important to avoid the dogmas and creative recipes that offer magical solutions. What is required to achieve the closing of the digital divide is pragmatism, private public dialogue, policies that expand the competitive market, reduce costs and favor investments, to which must be added policy instruments that complement this effort towards those less profitable areas.

13.6 The barrier of affordability

We have talked fundamentally about the instruments and policies to expand the supply of services. However, as is evident, many times

the problem that limits the adoption of the Internet is the income restriction associated with the lowest social strata of the population. In Latin America, the base of the pyramid comprises about 25.5 million households (some 116 million people), corresponding to the poorest sector of the population and with a household income of less than USD 250 per month, which means an important budget barrier for families to connect. According to a study published by cet.la in 2015[299], the purchase of a basic ICTs basket implies dedicating 12% of the monthly income for the population of the first decile and the complete basket[300] 32%, which makes it practically unaffordable.

Graph 7: Population Pyramid in LATAM.



Sources: Argentina (INDEC); Bolivia (Ministry of Planning and Development); Brazil (IBGE); Chile (Ministry of Planning through the Department of Economics of the University of Chile); Colombia (DANE); Ecuador (INEC); Mexico (INEGI); Peru (INEI); Uruguay (INE)

299 Katz (2016).

300 Typical consumer basket in the home: Basic: Defined as 2 smartphones with a cheaper voice and data plan, open TV and no broadband to computer. Complete Basket: 2 smart phones with cheaper voice and data plan, basic pay TV service, Internet connection via fixed broadband.

Table 1: Percentage allocated to ICTs services per basket in the first decile. Source: TAS.

País	Ingreso (moneda Local)	Ingreso (en US$)	Canasta 1	Canasta 2	Canasta 3	Canasta 4
Argentina	A$ 2.612	US$ 296	13,63%	30,44%	43,71%	50,10%
Bolivia	B$ 1.620	US$ 234	7,03%	12,16%	19,54%	25,71%
Brasil	R$ 811	US$ 250	10,91%	19,55%	29,60%	28,35%
Chile	C$ 217.891	US$ 349	10,75%	19,47%	27,40%	30,20%
Colombia	CO$483.219	US$ 193	16,73%	24,18%	36,75%	34,50%
Ecuador	US$ 213	US$ 213	19,74%	28,70%	47,61%	46,55%
México	M$ 3.458	US$ 233	13,59%	18,48%	31,55%	34,44%
Perú	S/ 927	US$ 303	11,02%	19,65%	28,31%	31,98%
Uruguay	U$ 10.611	US$ 406	7,87%	16,13%	22,29%	24,85%
LATAM	N/D	US$ 246	12,42%	20,40%	31,65%	32,11%

Sources: TAS

The affordability barrier presents a structural challenge, it persists despite a reduction in the prices of services in recent years, as a result of competition in the sector. This price reduction has markedly changed the market for telecommunications, with a lower inter-annual average of more than 8%. However, the challenges remain significant.

Table 2: Most economic plan for mobile services in LATAM.

País	2010	2015	TACC
Argentina	US$ 25,21	US$ 16,20	-8,46%
Bolivia	US$ 16,38	US$ 7,42	-14,65%
Brasil	US$ 19,31	US$ 11,40	-10,00%
Chile	US$ 29,58	US$ 14,71	-13,04%
Colombia	US$ 11,45	US$ 9,37	-3,93%
Ecuador	US$ 21,28	US$ 22,40	1,03%
México	US$ 19,57	US$ 15,35	-4,74%
Perú	US$ 27,84	US$ 12,37	-14,98%
Uruguay	US$ 10,91	US$ 7,83	-6,42%
Promedio regional	US$ 19,93	US$ 13,01	-8,17%

Note: Most economic plan with at least 1 GB per month of CAP
Source: CAF Ideal 2014 and Observatory of DIRSI prices

Although prices have fallen, the economic limitation for the acquisition of connectivity equipment (devices and terminals, such as smartphones or computers) in low income social contexts makes this barrier even more insurmountable. The complete basket continues representing between 25 and 50% of the monthly income of the households of the first decile in the region, a volume

of expenditure that is impossible to assume for these sectors that must prioritize other basic needs.

In order to face the income restriction of the base of the pyramid, it is necessary that companies have the flexibility to offer diverse commercial plans, to expand their range of services and to be able to adapt to the needs and capacities of payment of the different groups of users. But that is not enough. It is necessary to implement new policies on the part of the state, focused especially on the lowest income sectors of the population, aimed at removing the structural barriers for the adoption of new technologies and the experimentation of models alternative connectivity, as long as they do not generate counterproductive effects on investment. In this sense, the experiences implemented in some countries to reduce taxes and tariffs on services and terminals, as well as implement demand subsidies, account for the elasticity of demand to respond to the relaxation of family budget constraints.

One tool that governments have at hand to reduce the cost of services is the tax burden. In some countries, such as Brazil, over 40% of the final price of telecommunications services is explained by tax burdens of different nature. It is not a question of requesting tax exemptions or favorable treatments for telecommunications, but of correcting the fact that in many countries telecommunications services are excessively burdened.

13.7 Conclusions

To achieve the closing of the digital divide, it is essential that all actors adequately fulfill their role and that there is an adequate understanding of the role, the decision processes, and the restrictions faced by each one. Public-private dialogue plays a very important role in the construction of trust and the indispensable process of empathy with the different actors. The foregoing is not contradictory with heterodox initiatives to accelerate investment and network expansion processes, but it is fundamental to adopt the safeguards so that these initiatives effectively leverage the maximum possible expansion of the market and that they do not produce counterproductive effects. It is urgent to build an ambitious strategy among all the key actors to accelerate investment processes.

Closing the digital divide and achieving a world-class connectivity infrastructure is a necessary condition, but not enough to advance development. It is not enough to have access to networks, we have to turn Information and Communication Technologies into a strategic factor of productive transformation. In that sense, one of the most important challenges is the transition from a consumer Internet to an industrial internet. The digitalization of production processes and the assimilation of digital technologies in SMEs is an unavoidable need as a region. It is also essential for this transition, the assimilation of digital capabilities in present and future generations, where the role of education is fundamental. That is, there are many challenges beyond connectivity, but without connectivity it is impossible to even pretend to address them.

13.8 References

Banco Mundial (World Bank) (2016). World Development Report 2016: Digital Dividends. Washington, DC: World Bank. doi:10.1596/978-1-4648-0671-1.

Cáceres, R. B. (2011). Uso de los fondos de acceso universal de telecomunicaciones en países de América Latina y el Caribe. CEPAL. <https://repositorio.cepal.org/bitstream/handle/11362/3912/S2011088.pdf>.

Cet.la (2014). Desafío cet.la 2020. Inversiones para cerrar la brecha digital en Latinoamérica. Convergencia Research. <http://cet.la/estudios/cet-la/resumen-ejecutivo/>.

CIGI-Ipsos (2017). Global Survey on Internet Security and Trust. <https://www.cigionline.org/internet-survey>.

Frontier & cet.la (2017). Análisis de competencia en mercados dinámicos. <http://cet.la/estudios/cet-la/analisis-competencia-mercados-dinamicos/>.

Katz, R. (2016). Cet.la Iniciativas para el cierre de la Brecha Digital. Teleadvisory Group. <http://cet.la/estudios/cet-la/iniciativas-para-el-cierre-de-la-brecha-digital-en-america-latina/>.

Katz, R. (2015). El Ecosistema y la Economía Digital en América Latina <http://cet.la/estudios/cet-la/libro-el-ecosistema-y-la-economia-digital-en-america-latina/>.

14 A New Model for Increasing Access Infrastructure and Use of the Internet for an Inclusive Digital Society

Christoph Steck

Abstract

The availability of broadband infrastructure is one of the first requirements for people to access the Internet and enjoy digital services such as banking or access to online health services. It is also important for the development of companies, since digitization is fundamental for its operation and competitiveness. On the other hand, there is a part of the population that, even having access to this infrastructure, is not connected. Thus, it is necessary to address both problems in an aligned manner, both by the public sector and by the private sector, each in the exercise of their competences.

The private sector must innovate in technology and in business models in a way that allows it to make the infrastructure sustainable in areas where it is not today. Accordingly, the public sector must focus all of its actions on allowing sustainability to occur, while ensuring that regulations of another era do not prevent facing this challenge with guarantees.

Regarding the adoption of the Internet, the private sector must find new access marketing models, both in direct offers to users and in the exploitation of the double-sided market characteristic of the Internet, so that not all the economic burden falls on consumers, but is distributed throughout the entire value chain of digital services.

The public sector must pay attention to the digital training of the population, so that it is able to take advantage of the content and services offered to them. In addition, they must avoid using ICTs services as a direct source of income, since the economic impact for society of investments in the ICTs sector is greater due to the competitiveness factor that it adds.

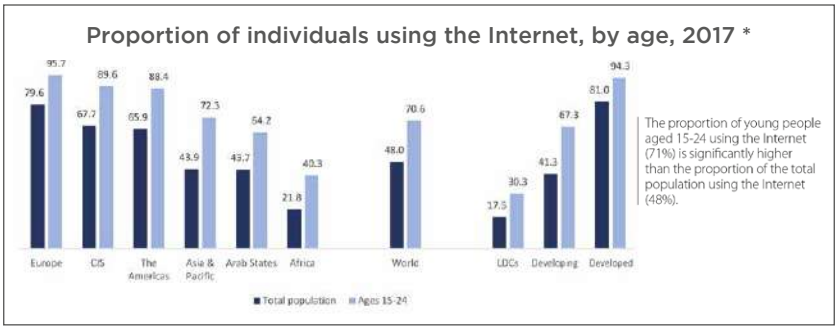
We are facing a digital revolution that is transforming society in a way and speed never seen before, and it is the

responsibility of the public sector and the private sector to make this process inclusive, leaving no one, wherever they are located, on the sidelines.

14.1 Introduction: The importance of being connected

The historical development of the Internet has created the most powerful transforming platform on earth. It is present in our lives both directly, when we use online services or provided directly on the Internet, and indirectly, using other offline services, where the Internet is a fundamental element of its operation, although this use is transparent to consumers.

In 2017, 50% of the world's population was already connected to the Internet – a historic breakthrough. According to the ITU[301] 67% of the population is connected in the Americas and 88.4% among young people between 17 and 24 years of age, which gives an idea of how important it is the Internet for our young population, who represent the future.



Source: ITU ICT *Facts and Figures* 2017.

This great progress, which happened in few years, has been achieved thanks to private investments. Telefónica has invested 45 billion euros in the last 5 years, 25 million euros a day[302]. With this impressive speed of growth, the Internet is allowing fundamental services such as banking or healthcare to reach everyone thanks to digitalization.

301 See ITU (2017).

302 See Telefonica (2017).

There is no doubt that one of the first requirements for people to access the Internet is the existence of infrastructure that allows it. It makes the difference between those who have access to it, and who therefore enjoy the advantages of digitization, and those who do not have this access and are therefore "disconnected".

In addition, connectivity must be sufficient, it is not enough that some online services work, but others do not. Connectivity should be good enough to enjoy all the services that the Internet can offer. Since these services are always demanding greater bandwidth and better quality, the effort investment and sustainability become decisive factors. Not only in rural areas which are difficult to access, but increasingly also in ultra-dense areas due to the demands of traffic concentration.

There is also a percentage of the population that, even with access to infrastructure, is not connected to the Internet for various reasons, such as[303]:

- they lack the basic digital skills and knowledge
- they do not need it for their daily life, or at least, so they believe that
- they do not find the Internet interesting
- they are not able to understand the revolution that is taking place through digitization, and therefore they cannot realize the need to be connected

The creation of connectivity infrastructures and the promotion of their use is, therefore, a double task both for the private sector and for the Public Administrations of the States, which must address both aspects of Internet access:

- the offer of access, both in the existence of the infrastructure itself and in the commercialization of it, and
- the demand for access, which ranges from stimulating demand through attractive content and services, to training the population in digital capacities.

303 See ITU (2017b).

14.2 Measures to favor the expansion of access infrastructure

14.2.1 The private sector

The investment effort made by the private sector to provide infrastructure for Internet access to society has been initially directed to areas where population density makes it easier to provide coverage to the greatest number of people. The use of always scarce resources, as well as the existence of necessary auxiliary infrastructure in the areas to be covered (mainly ducts, poles, and energy), made these areas the fastest and most sustainable ones to be undertaken.

Today it is necessary to provide access infrastructure to areas where basic civil infrastructures do not exist which may prove unsustainable. In these areas, the costs could exceed several times those of a more urbanized or less rural area, and it is intended that Internet access means a radical change for these populations. In those environments, mobile Internet hybrids between *backhaul* Wireless and fixed access without wires are shown as a very promising solutions.

To face these challenges, *stakeholders* of the private sector should work to lower the costs of creating access infrastructure, as well as lighten the burden of operating them. In this sense, Telefónica considers that the private sector should:

- develop equipment and innovative technical solutions to overcome the challenges presented by the current generation of equipment.
- find new business models that allow increasing the available resources, exploring the cooperation with other elements of the sector.
- work together with the supply chain of the access infrastructure to online service providers, cooperating with them to find sustainability in the required investments.
- completely transform and reform business models, as well as marketing models so that investments in new 5G networks can be developed not only where there is a strong demand.

- encourage the use of open technological standards, especially in the operation of networks, so that new exploitation models can be structured to lower its costs.

To be able to provide 5G in remote areas, it is essential that the operation of the networks be simplified as much as possible, since cooperation by the local society will be necessary for their operation; for example, taking charge of the maintenance of the equipment installed there or allowing private initiatives of local networks that can then be connected with other networks to achieve full operability.

In short, it will be necessary for the private sector to innovate in business models that allow it to face the challenge of providing access infrastructure anywhere, in a sustainable manner.

Firmly convinced that the challenge of connecting everything will not be solved by a single agent, Telefónica is also participating in other initiatives of interest groups and sectors such as Telecom Infra Project[304] and Loon Project[305] from Google X.

Public authorities should actively participate in these initiatives and support them as well.

14.2.2 The Public Sector

However, although private initiative has a way to go in regards to how networks are deployed, public administrations must also adapt to these extremely difficult environments. That is, private initiatives must be accompanied by other measures aimed at:

- encouraging risk-taking and innovation in the provision of infrastructure by modernizing digital policy and regulatory frameworks.
- including the broadband development in national digital agendas.
- planning and supplying spectrum efficiently and urgently.
- encouraging sustainable competition and a powerful local digital economy.

304 See <https://telecominfraproject.com/members/>.

305 See <https://x.company/loon/faq/#partners-section>.

14.2.2.1 Public Policy Modernization

It is essential that public policies stimulate the new wave of private investment in infrastructure, providing confidence and security to investors. The best practices and experiences[306] in recent years have shown the following:

- A **regulatory environment that rewards economic agents willing to take the risk is essential.** It must promote as well a sustainable competition model based on infrastructure for broadband.
- For the **remote geographical areas,** where private investments are not commercially viable, public-private partnerships (PPPs) have always shown superior results to pure public investments.

Initiatives with a holistic approach such as the "Gigabit Opportunity Zones"[307] of the FCC in the USA as well as the Spanish Broadband Extension Plan (PEBA)[308] are examples of the combination of fiscal incentives aimed at accelerating the expansion of coverage of ultra-high speed broadband networks in areas without current coverage, and where it is not expected in the medium term, granting subsidies to private companies that follow non-discriminatory competitive processes. The beneficiaries share the investment risk by committing a minimum percentage of the project investment that ranges between 45 and 60% depending on the characteristics of the project.

14.2.2.2 Digital Agenda

National digital agendas can play a decisive role in coordinating different public policies to expand the availability and use of the Internet. They comprise a series of issues such as broadband plans, policies related to the promotion of an open Internet, the strengthening of consumer rights or the setting of adequate taxation.

A comprehensive agenda should also encourage private investments to eliminate obstacles to the deployment of infrastructure, and adapt the spectrum policy to the possibility of connectivity in a given country.

306 See Feasey & Cave (2017).

307 See Pai (2016).

308 See Spain (2017).

However, it is essential when designing these national broadband plans that resources be allocated in a non-discriminatory and neutral way, from a technological perspective. Digital Agenda models in which technological options are limited to fixed services, mobile only or satellite only are less successful than those in which the operator can choose and combine any available technology.

14.2.2.3 Spectrum

The allocation of spectrum in a fair, efficient, timely and competitive manner and the availability of sufficient broadband spectrum are the oxygen of successful policies. The new challenges posed by the convergence of markets and, of course, the digitalization process, mean that we need 21st century regulation.

In this regard, it is necessary to release more spectrum in time for mobile use, particularly in emerging markets. Governments should also avoid fragmentation of the spectrum band among too many actors and avoid speculative investments in mobile spectrum licenses.

In addition, the more harmonized the allocated spectrum, the more economically viable will be the deployment of broadband networks due to the effects of access of scale to the network equipment.

Governments should give priority to coverage obligations on spectrum prices, noting that there will be compensation between the two. Better coverage leads to better economic results for the country than short financial gains to the State treasury.

Finally, it is necessary to pay attention to the duration and renewal conditions of spectrum licenses, since they are a determining factor in the certainty that the private sector needs to commit the high investments needed to build and / or modernize these infrastructures.

14.2.2.4 Same services, same rules, same taxes and user protection

Rapidly changing digital markets must be accompanied by regulatory modernization. All policy regimes around the world have implemented sector-specific regulation for telecommunications services, but today different agents interact and compete with

each other to provide an equivalent service to users. In the same way that it is widely accepted that consumers should have the same level of protection regardless of the company providing the service, so it must be agreed that such protection remains independent from the technologies used or the way in which the services are paid (money or personal data).

We must also modernize tax regimes and adapt them to the realities of the market. Despite the fact that high-speed networks have been identified as a key element for the development of the digital economy[309] and many governments recognize the role of broadband infrastructure for social development and economic growth, the tax treatment of the industry is not always fully aligned with the goal of connecting everyone.

14.3 Measures to favor the adoption of the Internet

As we said in the introduction, it is important to point out that even with broadband connectivity and devices available at affordable prices even for the poorest, around 20% of people do not access the Internet because they do not know how or do not see the need to do so. This was reflected in the study carried out by the International Telecommunication Union (ITU), in its report "Connecting the Unconnected"[310].

Thus, once the infrastructure is in place, and therefore users have the possibility to connect to the Internet, the following factors for adoption and use are relevant:

- **Affordability**, which includes both the cost of the Internet access service (broadband connection and data) and the necessary devices (smartphone, tablet, computer etc.).
- **Perception of value and digital literacy**. Social aspects that are often linked to the **lack of relevant content** in the language of the consumers, outside of their interests and local contents. This includes, but it's not restricted to services or contents that are not adapted to people with special needs.

309 See OECD (2017).

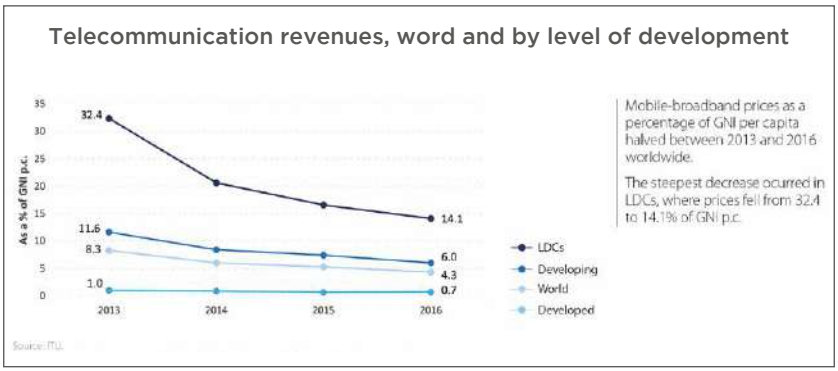
310 ITU (2017b).

14.3.1 Accessibility

The path to making access to infrastructure accessible through lower retail prices, which has been known as the "*glide path*" of pricing, has been completed already.

According to the ITU data for 2017, it has been observed that not only in developed countries, but also in developing countries, the price drop is generating a drop in income for those who build the Internet access infrastructures, which is a contradiction when, in addition, the Internet access service has been steadily growing in double-digits annually.

Income of the Telecommunications sector, global total and by level of development according to ITU[311].



Source: ITU ICT Facts and Figures 2017.

Thus, policy makers should avoid the use of investment in infrastructure as a source of tax revenue, since it can be a significant disincentive for the investment itself, as well as detract resources from the investment itself. The objectives of connecting everyone and generating tax revenues are antagonistic objectives in the Telecommunications sector.

This is the case of governments that tax on a greater scale broadband providers and consumers over other standard goods and services, sometimes even as luxury goods or services. The range of taxes applied is wide and it affects not only service providers, but also consumers: from taxes on the use and activations of mobiles, to

311 See ITU (2017).

taxes on terminals and devices, customs duties on imported phones, SIM cards, universal service obligation, spectrum rates or licenses.

According to the latest report of the GSMA on taxation[312] for a group of 30 developing countries, the payment of taxes and fees amounted to an estimated 29% of market revenues in 2014, of which one third are industry-specific taxes. According to this report, a 50% reduction in taxes and rates specific to the sector could potentially add around 140 million new connections over 5 years, an increase in market penetration of 5% with associated economic and social benefits.

In developing and emerging countries, where almost 30% of people still live in poverty[313], new formulas are needed to make the Internet accessible to all. Operators, on the other hand, must examine new models of commercialization and financing of infrastructures, and in the same way that we mentioned earlier in the measures to favor the supply of infrastructures, they must find innovative business models that facilitate the access of consumers to Internet.

An example of strategy followed by many operators are the offers at zero cost (better known as offers *Zero Rating* in mobile networks) in which consumers are allowed to access one or more Internet services without associated traffic being counted, therefore using more Internet for less (or the same) price, encouraging both the services that are under the format of *Zero Rating* and the rest, since consumer resources are released to use in the rest of the Internet, especially if the services *Zero Rated* are those that the consumer already uses more intensively, as recognized by the study on the offers of *Zero Rating* of the Directorate General for Competition of the European Commission[314].

Another example with great support from operators is the "*Network Slices*" in 5G networks, where the two-sided market nature of the Internet is exploited so as to not place all the economic effort on consumers only, but on the entire value chain of services.

312 GSMA (2016).

313 (World Bank).

314 European Commission (2017).

In relation to these private initiatives, the public sector must respond with courage and a holistic vision of the objectives pursued, adapting the regulations that, having been conceived for a traditional environment, are now overtaken by innovation. A clear example would be the caution at the time of applying rules of net neutrality, developed already in several countries of the continent, where a rigid application, not backed by empirical evidence, could prevent the aforementioned business models from being developed.

14.3.2 Perception of value and digital literacy. Relevant Content

The perception of Internet value and literacy, are fundamental to connect everyone, which leads us to recognize the need to focus on stimulating the creation of content and relevant services at the local level and the improvement of the set of digital skills.

In this field, the role of the public sector is key because of its ability to influence both through direct creation and through subsidies to other sectors. Thus, they should focus on:

- Promoting the creation of relevant content and services at the local level through the support of a start-up ecosystem adapted to local demand and able to compete globally. Supporting both digital skills training in schools, and in digital centers created ad hoc in which citizens can learn digital content skills, as well as more advanced skills such as coding and application programming.
- Development of e-Government services, which can greatly help to make Internet content relevant: tax collection, general administrative processes for people living in remote areas and reporting on the problems of cities, providing governments with tools to interact and get involved with local communities, while encouraging society to be connected.
- Finally, by implementing accessibility standards and an assisted digital strategy for people with special needs, including age and disabilities, we will reduce the digital divide and promote equal opportunities.

Creating content and services of local relevance and a start-up ecosystem is an area in which the private sector also has a relevant role, as (and let me speak about our company) Telefónica is doing by strongly supporting the entrepreneurial talent throughout Latin America, helping to turn innovative ideas into successful businesses thanks to our Telefónica Open Future program[315].

Furthermore, focusing on the creation of state-of-the-art audiovisual content in Spanish and Portuguese with Telefónica Studios, because language is also a fundamental requirement, especially for developing countries affected by the lack of content in the local language. 55% of Internet websites are in English and only between 20 and 25 % of the population speaks it (all over the world about 6.500 languages are spoken).

14.4 Conclusions

We are facing a digital revolution that is transforming society in a way and at a speed never seen and it is the responsibility of society itself to make this process inclusive, leaving no one, however difficult its location, on the sidelines.

The public sector has the unavoidable task of making this inclusion materialize, adopting a holistic vision of laws and regulations that consider the outcome for the end user, abandoning rigidities and dogmas of times in which the policies of these sectors were treated in isolation, with ad-hoc solutions that took years to implement and are being overwhelmed by the current reality.

The private sector also has to do its part, exploring, innovating, seeking imaginative solutions to the problems of financing networks. They must abandon old ways and open up to intersectional cooperation, collaboration with online service providers and to "coompete" with their peers.

315 See <https://www.openfuture.org/en/info/about>.

14.5 References

Comisión Europea. (2017). Zero-rating practices in broadband markets. <http://ec.europa.eu/competition/publications/reports/kd0217687enn.pdf>.

España (2017). Programa de Extensión de la Banda Ancha de Nueva Generación. Ministerio de Energía, Turismo y Agenda Digital. <http://www.minetad.gob.es/PortalAyudas/banda-ancha/Paginas/Index.aspx>.

Feasey, R. & Cave, M. (2017). Policy towards competition in high-speed broadband in Europe, in an age of vertical and horizontal integration and oligopolies. Centre on Regulation in Europe (CERRE). <http://www.cerre.eu/sites/cerre/files/170220_CERRE_BroadbandReport_Final.pdf>.

GSMA. (2016). Digital inclusion and mobile sector taxation 2016. The impacts of sector-specific taxes and fees on the affordability of mobile services. <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Digital-Inclusion-and-Mobile-Sector-Taxation-2016.pdf>.

Organización de Cooperación y Desarrollo Económico (OCDE). (2017). Key issues for digital transformation in the G20. Report prepared for a joint G20 German Presidency. OECD Conference. <https://www.oecd.org/g20/key-issues-for-digital-transformation-in-the-g20.pdf>.

Pai, A. (2016). Summary of FCC Commissioner Ajit Pai's Digital Empowerment Agenda. Federal Communications Commission. <https://apps.fcc.gov/edocs_public/attachmatch/DOC-341210A2.pdf>.

Telefonica. (2017). Conectar a los no conectados: cómo llevar Internet a todos. Public Policy. <https://tinyurl.com/ycqpjmsj>.

Unión Internacional de Telecomunicaciones (UIT). (2017). ICT Facts and Figures 2017. <https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx>.

Unión Internacional de Telecomunicaciones (UIT). (2017b). Connecting the Unconnected. Working together to achieve Connect 2020 Agenda Targets. <http://broadbandcommission.org/Documents/ITU_discussion-paper_Davos2017.pdf>.

Banco Mundial (World Bank). (2017). Poverty Overview. <http://www.worldbank.org/en/topic/poverty/overview>.

15 Expansion of Infrastructure and Internet access: The Experience of *Sustainable Villages for Development*

Filipe Batista **and** ***Nadine Chorão***

Abstract

In this chapter the project *Sustainable Villages for Development* (SV4D) will be presented, which was designed to promote digital inclusion through access to the Internet, taking into account the characteristics of the Community of Portuguese Language Countries Community (CPLP). This project, developed by the Association of Regulators of Communications and Telecommunications of the Community of Portuguese Language Countries (ARCTEL-CPLP), has now evolved in a partnership with the Research and Development Association – Fraunhofer. The central idea is to create a network of laboratories focused on the research and development of ICTs solutions for development, solutions to meet the needs of developing countries and within the framework of the competences of ARCTEL. This is a relevant issue in the field of development and universalization of communications services in places where there are greater sectoral deficiencies. From this objective, it is intended that this network create the necessary conditions for the promotion of local training, giving hypothesis for students from the technological areas, who can work in these laboratories and develop their ideas supported by the teams of ARCTEL and Fraunhofer.

15.1 Introduction

This chapter will present a project designed to promote digital inclusion through access to the Internet, taking into account the characteristics of the countries of the Community of Portuguese Language Countries (CPLP), which includes Angola, Brazil, Cape Verde, Guinea-Bissau, Equatorial Guinea, Mozambique, Portugal, Sao Tome and Principe and East Timor[316]. This project was prepared

316 See <https://www.cplp.org/>.

by the Association of Communications and Telecommunications Regulators of the Community of Portuguese Language Countries[317] (ARCTEL-CPLP), and it has now evolved in a partnership with the Research and Development Association – Fraunhofer[318].

ARCTEL-CPLP was created in 2009 with the objective of reinforcing the exchange of information among the various regulators that constitute it, thus contributing to the development of the market and the communications sector. Since its creation, ARCTEL-CPLP has been developing various studies to provide its members with tools that allow them to have a better and more effective regulatory activity. The studies were developed with the support and collaboration of the International Telecommunications Union, highlighting the Study on Universal Service and the study on Electronic Commerce. Specifically, these studies allowed ARCTEL to perceive that, regardless of the current work carried out to support the members, it was necessary to focus efforts on the development of specific projects that would reinforce our digital skills. In particular, to develop their societies aiming at their digitalization, also allowing to contribute to the development of the Digital Economy in the CPLP.

15.2 The project Sustainable *Villages for Development*

The issues of Internet access are the base of any digital economy. Therefore, for this purpose, to promote access to the Internet, ARCTEL-CPLP developed the project *Sustainable Villages for Development* (SV4D). However, more than simply enabling access, it is necessary to train and support populations to use access in a useful and beneficial way, promoting electronic governance and the use of online services.

Thus, the SV4D project was developed in the sense of combining access, with the diversified (or useful) use of the Internet and the universalization of the use of Information and Communication Technologies (ICT). A simple concept, but of complex implementation which involves the interaction of different actors. The objective is to build network laboratories in rural areas of 9

317 See <http://www.arctel-cplp.org/pt>.

318 See <https://www.fraunhofer.pt/en/fraunhofer_portugal/home.html>.

countries of the CPLP, which do not have access to broadband internet. It is intended to be sustainable and maintained without a foreseen conclusion, unless decided by the local managers. The central idea is to create a network of laboratories focused on the research and development of ICTs solutions for development, solutions to meet the needs of developing countries and within the framework of the competences of ARCTEL. This is a relevant issue in the field of development and universalization of communications services in places where there are greater sectoral deficiencies.

From this objective, it is intended that this network creates the necessary conditions for the promotion of local training, giving hypothesis to students from the technological areas to work in these laboratories and develop their ideas supported by the teams of ARCTEL and Fraunhofer. In addition to the research work to be carried out locally and individually in each village of the network, the idea is to allow the transmission of data between the different villages to accelerate eventual proof-of-concept tests of developing solutions. It adds concepts of Big Data Analytics operated by the collection of diverse information, in what refers to a wide range of topics such as meteorological phenomena, agricultural production, measurement of contamination, tracking of diseases, among others.

In addition to the central objective of creating a laboratory network, the concept of sustainability is based on alternative energy sources, with the entire communications structure and the laboratory itself being powered by clean energies, such as solar, wind and eventually the of water. In this way the local population (where the villages are installed) is allowed to benefit from access to clean energy, being able to add other benefits besides access to communications.

The central problem to be addressed concerns the need to promote the development and universalization of communications services. In particular, the issue of access to broadband Internet as a fundamental vehicle for development and economic growth. However, access by itself does not boost anything. It is necessary to ensure the development of projects and tools that promote the use of ICTs and add more value to local communities.

It is in this context that the project aims to include a set of online solutions that create visible benefits for communities where sustainable villages are installed. The e-health or e-education solutions will be developed to find and fill the gaps. Their results will be monitored and subsequently compared between the village network, in addition with other villages outside of this project. Finally, the creation of the laboratory network will enable the development of technology-based solutions aimed at development and allowing (by virtue of the network concept) the acceleration of tests and concept tests of the solutions to be developed.

At the same time, it will allow, at the election of local decision-makers, to focus on one or two priority areas in the field of applications. This process will also help to promote local entrepreneurship, leaving ARCTEL and Fraunhofer as responsible for evaluating the ideas and obtaining international financing for their materialization. In summary, the objectives of the project are to promote broadband Internet access and the universalization of technology-based services; createing a network concept that allows the transmission of data on a global scale; promoting the development of technology-based solutions for development and promoting the use of e-services.

In terms of results, what ARCTEL expect is to achieve in the medium term the reduction of areas without access to communications and ICTs, thus promoting universal access, improving the living conditions of local populations, and creating an accelerated system of development and testing of technology for development. Of course, the decision of the place of application depends on the responsibility of the authorities of each country. The idea is to reach rural (or fishing) isolated populations, of low income and without access to ICT, thus contributing to their development and support with ICT-based services.

15.3 WiBack System

The system selected to implement the project is WiBack system[319], is a Wi-Fi network that uses point-to-point direct beam connections

319 View <https://www.wiback.org/>.

(antenna to antenna). The maximum distance between two WiBack antennas is (with a required line of sight) of 20 km and a maximum of 10 antennas can be implanted in a row. You can design networks with star or tree topologies, however with a maximum limit of 100 antennas. WiBack network has Ethernet connectors on the antennas and spectrum band management within WiBack is compatible with a WiBack controller (one per network).

On the masts of WiBack antennas, additional access points can be installed that can use WiBack as transparent interconnection and offer connectivity to local users. The typical access points are either Wi-Fi (hotspots) and / or GSM (BTS, Base Transceiver Station). The size of the BTS can be very small (femto-cell, nano-cell), but it can also be standard GSM BTS (but it requires a lot of energy).

To connect the WiBack network to the Internet is simple, because WiBack controller also acts as a router and contains an input port for IP traffic. Therefore, either the controller is directly connected to an Internet Service Provider or ISP (Internet Service Provider) or the traffic is encapsulated through another network, which in a different location offers Internet access.

The GSM voice traffic (and data) is different, since all GSM BTS are linked to the BSC (Base Stations Controllers) and, together, form the BSS (Base Sub System). So to carry GSM in Wiback network, a logical connection with a mobile switching center (MSC) is necessary, which manages voice calls, SMS and connectivity with external voice (and data), networks (roaming partners, POTS, Internet). The connection between the MSC and the BTS is implemented by the *backbone* of the mobile operator, which may be a fixed network, or another radio network.

In particular, for the SV4D project and on how to connect WiBack network to the Internet and, optionally, to the networks of GSM operators, this can be done in three different ways.

15.4 Internet only connection

On some or all WiBack antennas, Wi-Fi Hotspots can be installed and WiBack Controller connects to the Internet through a mobile operator's network. In this case the controller and the first WiBack

antenna must be installed on the mast of a GSM operator as close to the town as possible. The connection of the controller to the operator's backbone will be done by Ethernet / IP and later the traffic needs to be routed to the Internet, being necessary to define who will be able to do it and in what way that cost will be supported.

This option has the advantages of being very simple, low cost and with minimum energy consumption. The disadvantages are that most people in rural areas, today only have GSM phones; thus, the network will be under-utilized, used only by those with more sophisticated phones or more experienced users.

Internet Only

Source: Prepared by the author.

15.5 GSM and Internet connection

The second option is through the GSM connection and the Internet, using the BTS of the operators. Here Internet connects in the same way as described in the previous option, adding that the GSM BTS are mounted in one or more positions of WiBack network.

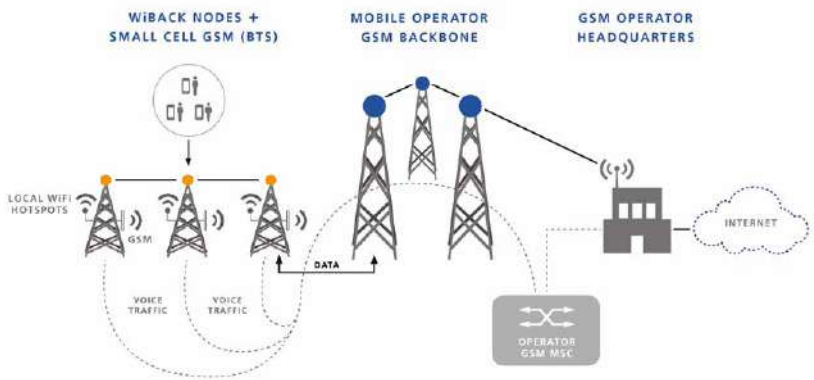
The BTS are connected to an operator's BSC through WiBack network, thus becoming part of the operator's network.

The main advantages of this option are that it remains a simple and low-cost solution, creating a GSM solution that is available to users in rural areas. In addition, if femto / nano-BTS are used, the energy consumption is also low.

The main disadvantages are that the operator has to maintain the femto / nano-BTS, or install the same model of BTS used in the

normal GSM network (potentially with high power consumption and high equipment cost). The problem can be multiplied if there is more than one operator interested in covering the deployment area (which may require two ERBs per antenna of WiBack network).

Internet GSM Voice: Operator Managed GSM BTS

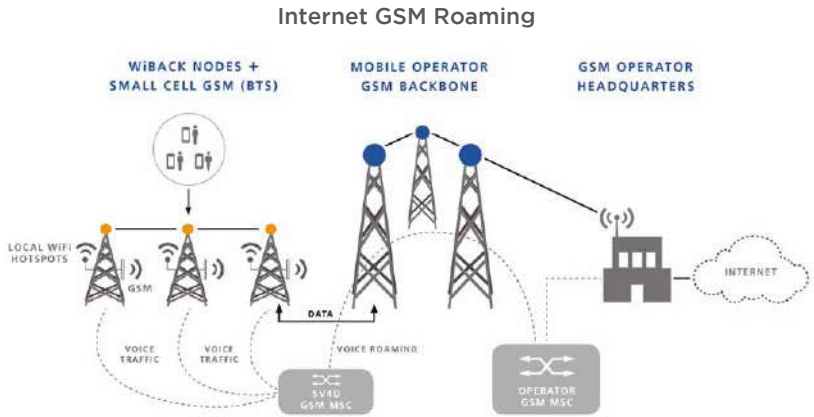


Source: Prepared by the author.

15.6 Combination of GSM and Internet

The third option is a combination of the previous ones (GSM and Internet) in which the person responsible for the management of Wiback will function as a roaming partner. Here the Internet connection is made as described in the first option and also a GSM BTS must be mounted in one or more places in WiBack network. BTS connects to a BSS of SV4D and MSC. All traffic (voice and data) is forwarded through the operator's network to the locations of interconnection (MSC of the operators) and voice traffic is inserted in the POTS / MSC.

The advantages are that we have total control of all traffic within the SV4D network, where free GSM calls within the SV4D network are possible, potentially also among all SV4D networks. The disadvantages are that we have an implementation project, compared to the previous ones, more complex and the new network or the SV4D becomes a GSM operator and will require a roaming agreement with commercial operators for connections outside the SV4D network.



Source: Prepared by the author.

15.7 Conclusions

This project is framed, along with a wide range of other initiatives, in the Digital Agenda for the CPLP. This initiative, approved its creation by the Meeting of Ministers of the CPLP in August 2016, in Maputo, Mozambique, has as main objective to align the digital strategies of the members of the CPLP.

The study of the Digital Agenda, carried out with the support of ITU, will be published in 2018. This study allowed gathering diverse information on the Communications and ICTs sector in the member countries of the CPLP, as well as drawing several conclusions and analysis of the state of the art in this sector. It has also made it possible to gather a broad set of legislative and statistical information that, from now on will be a solid base of acquis for the follow-up of the measures and their progress, which are derived from the strategies identified and presented in the Digital Agenda proposal for the CPLP.

Of the various readings and conclusions that can be drawn, the main one, and most natural, is that the CPLP brings together a group of members with different social, economic and political conditions. This diversity is, moreover, clearly present in the field of digital areas, where a group of countries with different factors is perfectly identifiable, thus generating a situation of “two” or “three” speeds “in the digital field of the CPLP. For this reason, the SV4D project,

which adapts to the reality of the country where it is implemented, is relevant from the point of view of the contribution it provides to raise awareness of the importance of the digital economy.

Therefore, it is undeniable that the starting point of each member state of the CPLP in the construction of its own digital agenda is different, which generates challenges, but, above all, opportunities, to the extent that certain stages of development can be avoided by countries with greater shortcomings in this area. The SV4D project is only one piece in the puzzle for the development of the Digital Economy and the Digital Agenda for the CPLP, which will allow and reinforce cooperation processes among the members, but will serve as a driving force for the development of other sectors.

This whole process is based on three axes of common digital forces within the CPLP: the common language and the similar culture, these aspects being immaterial, which contribute (and much) to the digital proximity between these countries; The legal and regulatory framework is (with some exceptions) quite similar and derives from a common legal tradition, which facilitates the legal approximation between the countries of the CPLP; and the existence of various Policies and Initiatives in the digital domain that present similar objectives, contents and measures in various countries, thus providing the conditions for greater proximity among the member states in the CPLP.

The main challenge that we intend to overcome, and whose contribution of the SV4D project is fundamental, refers to digital points of remoteness within the CPLP, such as the lack of a common market or integrated within the CPLP. Absent freedom of movement of people, goods and capital, or the lack of specific competences of the CPLP in the digital domain and the lack of application capacity. However, in this area, the ARCTEL-CPLP has made considerable efforts through the ARCTEL Training Center to expand the capacity and the creation of competences to combat the lack of digital education.

The experience of ARCTEL-CPLP and in particular the SV4D project, can be perfectly adapted to the reality of Latin America, where we are an integral part through Brazil.

15.8 References

ARCTEL, 2016, Anuário das Comunicações da CPLP, disponível em: <http://www.arctel-cplp.org/publicacoes>.

UIT-ARCTEL, 2015, Estudo sobre o Serviço Universal de Telecomunicações na Comunidade dos Países de Língua Portuguesa e em Macau, China. Disponível em: <http://www.arctel-cplp.org/app/uploads/publicacoes/13546896265a47d5f2e47e4.pdf>.

16 Weaving Technological Autonomy in Indigenous Peoples: Community Cellular telephony in Oaxaca, Mexico

Carlos F. Baca-Feldman*, *Erick Huerta Velázquez*, *María Álvarez Malvido*, *Daniela Parra Hinojosa* and *Karla Velasco Ramos

Note: this work is based on Huerta, E. and Bloom, P. (2017). *Manual of Community Cellular Telephony. Connecting to the next billion. Mexico: Networks for Diversity, Equity and Sustainability AC*

Abstract

Since 2013, Oaxacan indigenous communities in Mexico have generated a rupture in the radio spectrum. The creation of the first community cellular telephone networks in the world has triggered a process that disrupts the traditional organizational forms of telecommunications. This is thanks to the collaboration of native communities and hackers, supported by two social organizations (Rhizomatica and REDES A.C.). Later, in 2016, the emergence of Community Indigenous Telecommunications A.C.[320] allowed the consolidation of a project in which, for the first time, the communities themselves own and operate their own community networks that offer mobile phone services. The particularity of this experience lies in the legal, technological, economic, and organizational foundations of a model based on the notion of spectrum as a common good that is capable of helping considerably to connect the next billion in a sustainable manner. In this paper we describe and analyze these characteristics, together with their contextual dimensions, to understand the possibilities, limits and contradictions of this form of technological appropriation.

16.1 Introduction

In 2013, in Talea de Castro, Oaxaca, the first community cellular telephone network was installed in Mexico. The transformation brought about by this experience had a significant impact on the

320 See <https://www.tic-ac.org/>.

way in which technological autonomy is understood and weaved in indigenous peoples and rural communities around the world.

The creation of these networks started from a shared dream between two organizations that for several years have accompanied experiences of community and indigenous communication in Mexico and other parts of the world: Rhizomatica[321] and Networks for Diversity, Equity and Sustainability AC[322].

It was not only the promotion of connectivity in remote areas or a way of getting the possibilities, limits and contradictions of mobile telephony to these places, but rather a process of consolidation in the practice of the need to understand the radio spectrum as a common good. Today there are 22 communities in Oaxaca that have decided to create their own community networks and the expansion aims in the coming years to reach other states in the country.

In spite of the importance that the process of incidence has had in the regulatory policies of telecommunications in Mexico and that already resonates in other countries of Latin America, Asia and Africa[323], the core of this experience has been the concretion of a project that improves the autonomy of the indigenous towns and rural communities. The model is made up of a network fully operated and managed by the community. The role of Community Indigenous Telecommunications AC (TIC AC) and the organizations that make up the association of operators is to provide advice and develop technological improvements. By not having a single owner of the infrastructure, nor establishing a hierarchical structure in decision-making, what is pointed out in the model is the premise that the spectrum should be understood as a common good. How can one achieve this? From the community base, supported by the organizational, technological and economic bases of the model, as well as in the elements of the legal framework. In this sense, this article explores an alternative model of connectivity in which local communities are the actors that drive, develop and, of course, benefit from access to Information and Communication Technologies (ICTs).

321 See <https://www.rhizomatica.org/>.

322 See <https://www.redesac.org.mx/>.

323 For more information, see Rey-Moreno (2017) and Belli (2017).

16.2 The context in which these networks arise

The context in which this experience has been generated is framed within the limitations of the State and the capital that cause access to services and ICTs to be determined by the interests of the market, which produces a gap that is difficult to correct for those communities whose number of inhabitants is not enough for the investment in infrastructure of large telecommunications companies. Statistics on Internet access and telecommunications in Mexico, methodological issues that may provide higher results than what happens in reality[324], help us to perceive the dimensions of the disconnection in the country. In 2016, according to the *National Survey on Availability and Use of Information Technologies in Households* (ENDUTIH), developed by *the National Institute of Statistics, Geography and Informatics* (INEGI, 2016), 47% of citizens use a computer, 59.5% are Internet users and 73.6% have cell phones. These figures become even lower in states such as Chiapas, Guerrero and Oaxaca with a high index of indigenous populations.

As we can observe in these figures, technology is not neutral. It involves a series purposes and ways of functioning that frame the reality of a certain era. As a dialectical process in society, it is *in, against and beyond* of the market and the State (Holloway, 2011). Today technology aims, above all, but not only, at reinforcing the mechanisms of penetration of capital in the reproduction of life. As Manuel Castells points out (2002: 110):

> Technology is a fundamental dimension of social change. Societies evolve and are transformed through a complex interaction of cultural, economic, political and technological factors. It is therefore necessary to understand technology within this multidimensional matrix. All in all, technology has its own dynamics. The type of technology that develops and diffuses in a certain society decisively shapes its material structure.

324 An analysis of the methodology used by the government in Mexico to collect data on Internet connectivity is the study *The lug of Mexico connected* that developed the Network for the Defense of Digital Rights, written by Ortiz Freuler (2017).

Therefore, the enclosure at a technological level that we are living (Boyle, 2006), has not been an impediment for communities around the world, as they have decided to generate their own telecommunications projects in order to meet the needs of the disconnection, but with a construction and from processes that are woven from their own political, economic, social and cultural forms. In this way, beyond the projects promoted by the State, the communities themselves appropriate, transform and (re) signify the technologies so that they really become tools of their processes of social transformation.

As an example, in a doctoral research that is in the process of being carried out, Ernesto Cabrera, a graduate student in Sociology at BUAP, has found in nineteenth-century newspapers one of the first experiences of this kind[325]. According to the data collected, when the government of the United States decides to populate the Mississippi river basin, the villagers face the problem of delimiting their lands, which lead them to invent barbed wire to mark their properties. A few years later, with the arrival of the telephone to the east coast and the little disposition of the *Bell Telephone Company* to serve these communities that would not generate profits, an invention is created. They used the barbed wire as telephone cables and as a means to transmit music and news, and little by little they improved their devices so that they could have better reception. Probably this fact is the first experience of a community solution to the problem of connectivity through telecommunications. The technology that was designed to enclose private property was the same that allowed us to weave threads of communication between the people who lived there.

In this sense, in the *Toolbox of Best Practices and Policy Recommendations, Module 3ICTsfor Indigenous Peoples and Communities* (ITU 2011), the only successful projects in the promotion of connectivity in remote areas of Mexico are those in which decision-making and operation in the last mile networks come from the communities themselves.

325 At the moment this investigation is in preparation, so it will be published in the following months.

16.3 What are community cellular telephone networks?

In seeking the common as a central element for the reproduction of life, community cellular networks were characterized by the emergence of two types of communities: indigenous peoples and hackers of Oaxaca. On the one hand, commonality, as it was named for the lifestyle itself in the mountains of Oaxaca (Maldonado, 2015), contains characteristic elements that distinguish these communities from other indigenous peoples in some dimensions. Specifically, it is important to emphasize that what enabled the process of technological appropriation through community cellular networks has to do with the notion of autonomy, the collection system and the common goods that support these communities (Bloom, 2015).

The axes of commonality, following the systematization presented by Martínez Luna (2013: 269), are the territory as an integral relation between space and the species that inhabit it; the political form of organization based on the assembly and the collection system; the collective work that takes shape in processes like tequio and mano vuelta; and the party as an expression of the fruits of community work. All this in a constant process of tensions and possibilities that are woven around our own and others. As he points out:

> The daily confrontation of these two forces (imposition and resistance) generates agreements, that is, adjustments, both from the imposition and from the resistance. The social "harmony" is explained in agreements, in which both parties give up their pretensions [...] At the party, a son is danced the same as a cumbia and we must recognize that the son is also an adaptation [...] The megaphone, the amplifier, the console appear and dances are made with shrill sounds and wind bands.

Technologies, in experiences such as the one described here, are linked to these forms of adaptation, not by way of imposition but by appropriation and meaning, always taking as a fundamental element the self-determination processes of the communities. In this sense, the *hackers,* in this process of knowledge sharing for

the consolidation of these networks, have been able to shape the codification of *software* and creation of *hardware* necessary. The project has sought from the beginning the coding accessible to the users of the closed technology of the GSM through *free software*. This community is inserted in this experience because they share the organizational logics of collective work that allows them to approach the foundations of the *commonality*. As pointed out by Laval and Dardot (2015: 195):

> A "hacker", a term that designates both a passionate programmer and someone gifted for computing, would not be a lone wolf acting on its own, nor a simple *geek* worried only about the performance of his machine. The *hacker ethics*, as it is exposed in a certain number of works, has several dimensions. It is based on certain *ethos* of joy, a commitment in favor of freedom, a relationship with the community oriented towards the "generalized gift".

Taking as a starting point the relationship between these two communities, the process has been supported by two organizations that have served as a kind of umbrella for the realization of the project. On the one hand, Rhizomatica has been linked to the efforts made by *hackers* around the world, like the *OpenBSC*[326] in Germany and the *OpenBTS*[327] in the United States, for the creation of the technological model and the tools of *software* and *hardware* necessary to achieve the model. Likewise, in the beginning they were in charge of the implementation and operation of the model in the communities that wanted to be part of the network. On the other hand, Networks for Diversity, Equity and Sustainability AC designed the necessary legal framework and followed up on some evaluation and systematization processes of the experience. As of July 2016, under Communiqué 73/2016 of the Federal Institute of Telecommunications (IFT), the rural and indigenous populations of Mexico have their own telecommunications concessionaire, under the legal and operational figure of Indigenous Community Telecommunications.

326 See <http://openbsc.osmocom.org/trac/>.

327 See <http://openbts.org/>.

AC (TIC AC). Thus, in addition to the three major cell phone companies, Telcel, AT & T and Telefónica Movistar, TIC AC is located. The concession granted allows the expansion of the network in six states of the country, which places TIC AC in an expansion process and consolidation of this project in other territories.

Through these processes, the first community cellular telephony network began operating in 2013, but it was not until 2014 that the IFT authorized an experimental concession in the 850 MGHz band. This request to the Mexican government, beyond being a possibility to establish evidence on the operation of certain technological devices, sought to test the possibility of generating a telecommunications model with organizational forms and policies of the indigenous communities. In other words, the intention was to lay the necessary foundations for the consolidation of autonomous cellular telephone networks that were not limited to market norms and the State. This laid the groundwork for a legal framework that broke into public policy by generating the first mobile telephony concession for social use in the world.

Next, each of the constituent elements of the network is described.

16.4 The legal context

The legal model that sustains this experience is composed of two elements: the internal self-regulation norms, in each of the communities that operate a network, and the external norms that are made up of laws and regulations. In order to understand the legal framework as a whole, we have used the layer model of Yochai Benkler (in Lessig, 2001): physics, logic or code, and information. Depending on the type of network, each of them can be free or have restrictions.

The physical layer is divided into three. The first of these, the local network, is in the 850 MGHz band and consists of a radio base from which the community owns and is administered as a cooperative in which the community members are partners. The legal support of this layer comes from Article 2 of the Constitution and Convention 169 of the International Labor Organization (ILO) that indicate that indigenous peoples have the capacity to

design and execute their own regulatory systems. In Mexico this is recognized under the legal figure of *customs and habits* in which the powers of the State are delegated to the traditional ways of doing politics (Bravo, 2009). The transport network complies with the network of Wi-Fi links, and, although the spectrum is free to use, the system belongs to a regional ISP. Normally in this layer services of small commercial operators that already work in the area are subcontracted. The backbone network is linked with a public telecommunications network and has a closed code.

On the other hand, the association is made up of people and communities interested in the installation, operation or improvement of community cellular telephone networks in the country. Communities can become operators through the expression of this desire and with the consensus of their assemblies and authorities. The figures taken by each of the partners are that of technicians, operators, pre-operators or sympathizers. The partners, depending on their type of affiliation, will have different responsibilities and will have to abide by the constitutive rules of the association derived from the consensus in its governing bodies.

16.5 Technological base

The principles guiding the technological dimensions of this experience are the ease of operating the equipment so that the maintenance can occur directly in each community, and the low price of infrastructure so that 100 families can afford it without problems (approximately 5,000 USD).

The technology used is SDR (from English *Software Defined Radio*) or Radio Defined by Software, which transforms some of the elements of the *hardware* of a radio communication system to *software* so they can be used in a computer. Also, GNU Radio is used, a *software* that allows the implementation of radio systems at low cost and is normally used in experimental environments. These two inventions led to projects that managed to transform the closed technology of GSM into an open one based on what is known as "reversible engineering", like the aforementioned *OpenBSC* and *OpenBTS*.

The *software that makes up the network is itself made up of several previously* designed computer programs: OpenBCS, Linux Call Router, Freeswitch and Kannel. In addition to this, Rhizomatica has created customized packages. On the one hand, *Remote Application Programming Interface* (RCCN), allows executing all the components of the *software* on the whole. On the other hand, Rhizomatica Mobile community network is the open source repository of the entire operation of the network[328]. Finally, an administration interface has also been generated so that operators can access it through the http protocol.

16.6 Economic basis

In the architecture model of the economy, Braudel (1980) identifies three levels, each with its own institutions: the world economy, the local economy or the market economy, and the subsistence economy. For him, the fact that the subsistence economy is regulated through public policies as if it were the global one is the most common mistake. For this reason, telecommunications projects in rural areas generated outside communities often fail to consolidate.

In this way, taking into account the recommendations of this author, in the case of community cellular telephony, each element of the network has a model of its own organization according to the type of economy in which it operates. So the local network that operates in a subsistence economy is managed by the community, the transport network is operated by a local company and, finally, the backbone network is served by a global company. At the same time, in this model the community is part of an association that is capable of dealing in a global economy given its integration.

On the other hand, with respect to the costs and revenues of the services provided, the communities charge users 40 pesos monthly (around 2 USD). Of that amount, 25 pesos remain in the community and they administer it themselves and 15 pesos are allocated to the association for technical, legal and advisory services. All calls and text messages are free within the network. For calls abroad, the voice over Internet Protocol (VoIP) is used, provided by the Internet access provider that allows access to the global telephony network.

328 View <https://wiki.rhizomatica.org/index.php/Main_Page>.

16.7 Organizational basis

As we have indicated above, the organization takes as a basis the indigenous way of life. In this sense, it has been determined that the way in which the network mainly operates in regards to the collective and consensual decision of each one of the communities and actors involved. For this, three axes have been established in which the functions are developed.

The main dimension of this characteristic resides in each of the local networks, which are organized and managed from the decisions in the general assembly of each community. So each of the local operators has the ability to decide who will operate their network and how. For example, in the community of San Ildefonso Villa Alta, although the person in charge is the municipal secretary, the entire council is aware of the management of its cellular telephone network.

This is narrated by Ildefonso Alcántara in the following way, in a personal interview of 2015:

> We all had the responsibility. All of them. Always for anything of Rhizomatica we had to do a session of Cabildo, then we said that we were all responsible, nothing more than those that were more constant, maybe because we learned a little bit faster about the system and that was the secretary and me.

In the association as a whole, the governance structure is composed of an organ for decision making and an executive body. Decision--making is carried out through the assembly of associates in which all the operating partners and technical partners participate. In turn, the executive body is made up of two representatives of the operating partners and two of the technical partners, appointed by the general assembly and are responsible for shaping the decisions and guidelines that are generated in the assembly.

Additionally, the substantive areas in the organization are divided into three. The first of these is the operation, where all the elements for daily operation and the improvements required in each of the networks are developed, both in the deployment of the network,

as well as technical support and computer development. The second refers to the connection with the communities. The goal is to specify a network of networks because the network architecture is made up of the conjunction of each of the private networks in the communities. In the third, the central component is innovation, which is carried out based on collective work between the members of the association and other external organizations such as universities, *hackers*, researchers and people curious about technology.

Also, there are supporting areas, specifically with regard to administration and finance and regulation. The first of them is responsible for the entire accounting process of income and expenses of the association as a whole. The second's objective is to establish mechanisms for advocacy and dialogue with the authorities so that the legal model that accompanies the association can continue to develop. Both areas are not directly within the association's staff, but are services provided by external organizations.

16.8 Conclusions: challenges, limits and possibilities

The deepest dimension in the analysis of the future of community cellular telephony networks has to do with continuing to consolidate ruptures and transformations based on the logic and community bases that underpin the project as a whole. This can only be achieved by focusing attention on those processes that occur within each community and providing the tools that aim to solve the specific problems they face.

Thus, although cellular telephony has brought many benefits to communities, it has also expressed the deepest conflicts in the social relations that occur within them -- issues such as gender inequality, conservation of traditional values, power relations based on age etc. They have been key in the process. For example, in the case of the use that children of Talea de Castro give to cell phones, Israel, one of these children, commented in a personal interview in 2015:

> At the beginning of this, it was opened to the public. It did not matter if he was a boy, a young man, an adult. Then there came a moment when we started to think,

> really, a child, what will he use a telephone for? We did not want to make them consumers, or at least we had that idea, because many parents started buying their children's phones. Why should there be an expense to give a child a phone if they do not really need it? [...] Then we ourselves created that limitation, that there would not be users of telephony under 16 years.

Despite the challenges involved in creating these networks, the benefits have also been an important factor for more communities join the network. Keyla Maulemeth, in charge of the Talea GSM Network, summarizes the importance that this project has had in her community:

> It is the option if you have a community that is stuck in a mountain or that is in a region where there is no other system [...] First, because if you are a small community large companies will not give you the service, they are very expensive and a community like that does not have the resources to pay for it. Second, because if your own government does not support you to have a service even if it is part of your rights, you have to look for another alternative. Third, because it is economical compared to a Movistar team, for example: The Community Cell Phone antenna is three times cheaper. Fourth, calls are very cheap. Fifth, because you can build a collective and it is a project that is done for the community, it helps to activate the economy, maybe you can give one or two jobs and all the money generated is going to stay in the community and circulate there. Finally, it gives you autonomy, capacity and power to do what your local, state or federal government does not give you. Together and organized we can do it without needing to ask anything from anyone else (in Álvarez, 2017).

On the other hand, the challenges that are approaching in the work that TIC A.C. and its sister organizations are currently carrying out are related to the development and potentialization of the technological, economic, organizational and legal battles. An example being the expansion of the network to six states of the country.

At a technological level, a great challenge remains: the possibility of generating tools from the already consolidated bases. For this, we are working on the design of an instant messaging system (similar to WhatsApp or Telegram) for communication to the interior and exterior of the network. In addition, work is needed to strengthen user attention and the capacity of the network to avoid saturation, especially from the increase in the number of users and the use of devices more continuously. This is a constant concern, as the Ex-President of Villa Alta points out in a personal interview in 2015:

> The community, we can say, is already dependent on the cell phone. If the service is suspended, inadvertently, due to lack of knowledge, due to the lack of experience of those who are there now, people get worried, they ask themselves is happening, we have no signal, and we cannot communicate. They worry as if the cell phone was a water or electric service.

On the other hand, at a legal level, greater commitment from all stakeholders is required for the implementation of policies that benefit telecommunications projects such as the one described here. For example, although the concession has already been granted, in the last few months TIC AC has had to face legal proceedings due to excessive charges for the use of the spectrum that contradict the social use of the association. Likewise, in the economic aspect, it is necessary to generate funds that support more organizations to develop similar projects from their piloting until their consolidation, as well as for the research and creation of *software* and tools that allow low-cost access to telecommunications.

The path that the Oaxacan indigenous communities have started is one more step in the construction of technological autonomy from the villages. There is still a long way to go and there are many questions to answer them. In general, we agree with Zibechi's proposal when he points out that it is "*make community* instead of *be a community*"(2015: 76). In other words, it is a never-ending path that must be continually followed.

This experience conveys that there are other ways of organizing ourselves, of going beyond the limits and contradictions of the State and capital to solve technological problems. The answer has always been in work and collective dialogue.

16.9 References

Álvarez, M. (2017, Febrero 19). Telefonía celular indígena. Nuevo paradigma de comunicación. Nexos. Recuperado el 13 de enero de 2018, de <https://cultura.nexos.com.mx/?p=12170>.

Belli, L. (Ed.) (2017). Community networks: the Internet by the people, for the people. Official Outcome of the UN IGF Dynamic Coalition on Community Connectivity. Rio de Janeiro. FGV Direito Rio.

Bloom, P. (2015). La Telefonía Celular Comunitaria como Alternativa al Sistema Hegemónico de las Comunicaciones en México: Un estudio de caso de las nuevas iniciativas de la Sierra Juárez de Oaxaca. [Tesis de maestría no publicada]. México: UAM-X.

Braudel, F. (1980). On History. Chicago: The University of Chicago Press.

Castells, M. (2002). Epílogo: Informacionalismo y la sociedad en red. En P. Himanen, La ética del hacker y el espíritu de la era de la información (págs. 110-124). Barcenola: Destino.

Hayes, L. (2018). Farmer Mod from the 1800s – The Barbed Wire Phone Line. <http://georgia.growingamerica.com/features/2018/02/farmer-mod-1800s-barbed-wire-phone-line>.

Holloway, J. (2011). Agrietar el capitalismo. Puebla: BUAP.

INEGI. (2016). Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH). México.

International Telecommunications Union (ITU). (2011). Toolbox of best practices and policy recommendations, Module 3ICTsfor indigenous peoples and communities.

Laval, C., & Dardot, P. (2015). Común. Ensayo sobre la revolución en el siglo. Barcelona: Gedisa Editores.

Lessig, L. (2004). Introducción. En R. Stallman, Software libre para una sociedad libre (págs. 11-15). Madrid: Traficantes de Sueños.

Maldonado, B. (2015). Perspectivas de la comunalidad en los pueblos indígenas de Oaxaca. Bajo el Volcán(23), 151-170.

Martínez Luna, J. (2013). Textos sobre el camino andado (Vol. I). Oaxaca: CSEIIO.

Ortíz Freuler, J. (2016). El Estirón de México Conectado. ¿Cuánto creció realmente el número de usuarios de Internet? R3D Red de Defensa de los Derechos Digitales. <https://r3d.mx/2017/03/12/el-estiron-de-mexico-conectado-cuanto-crecio-realmente-el-numero-de-usuarios-de-internet-en-2015/>.

Rey-Moreno, C. (2017). “Supporting the Creation and Scalability of Affordable Access Solutions: Understanding Community Networks in Africa”. Internet Society. <https://www.internetsociety.org/resources/doc/2017/supporting-the-creation-and-scalability-of-affordable-access-solutions-understanding-community-networks-in-africa/>.

Zibechi, R. (2015). Collective works as material / symbolic common goods. The Apantle. Community Studies Magazine(1), 73-97

THE CHALLENGES OF PRIVACY AND CYBER SECURITY

17 A Profile of the new Brazilian General Data Protection Law

Danilo Doneda **and** ***Laura Schertel Mendes***

Abstract

This article aims to analyze the importance of the new General Data Protection Law (LGPD – Law 13.709 / 2018) to guarantee the rights of Brazilians in the 21st century and how the sanction of the Law consolidated a normative framework for the information society, complementing and dialoguing with other rules of the national legal system. It analyzes the main axes of LGPD, with particular emphasis on principles and rights contained therein. Finally, it examines the main challenges for LGPD implementation in the country.

17.1 Introduction

The last ten years have been of intense legislative activity on the subject of personal data protection in Latin America. During this period, many countries in the region adopted or began to consider adopting legislation regarding this issue. On August 14 of 2018, Brazil, the country with the largest population in the region, adopted its first General Data Protection Law – Law 13,709 of 2018, referenced as LGPD.

Brazilian law has a peculiar trajectory in relation to other Latin American data protection laws. Sanctioned in the same year as the entry into force of the European General Data Protection Regulation (GDPR) and the revision of Council of Europe Convention 108, it is one of the first regulations in the region to have the most direct influence of the GDPR, at the same time it also strongly reflects particular characteristics of the Brazilian legal system. These elements of governance derive directly from the way it was drafted since its inception.

Brazil was largely absent from data protection debates until a relatively recent period, apart from some exceptions such as bills proposed in the 1970s and 1980s that did not thrive. Even if the Federal Constitution of 1988 provides for the right to privacy as

well as the Habeas Data action, there has not been a concrete movement in the country to receive trends in data protection, at least until the middle of the 2000s.

Around 2005, when the Brazilian government was asked to respond, in Mercosur forums, to a proposal for a regulation on the protection of personal data, a formal debate began, initially restricted to the Brazilian government, regarding a possible solution legislation on data protection for the country's planning.

It was only in 2010, however, that the issue was addressed more broadly by government and society. In December of that year, the Ministry of Justice made public a first version of the Draft Law on Data Protection in a public debate held entirely on the Internet. This draft was sent to another public debate in 2015 and afterwards sent to National Congress for deliberations, until it was utterly voted and enacted, becoming law in 2018.

The General Data Protection Law (LGPD) thus introduced a general regime for the protection of personal data in Brazil, complementing the Brazilian regulatory framework of the Information Society, together with the Access to Information Law, the Internet Civil Rights Framework ('*Marco Civil da Internet*") and the Consumer Defense Code, the normative set that modernizes the treatment of information in Brazil.

By reflecting on the main influences that shaped the LGPD, it is possible to verify that it is inspired conceptually by the European model of protection of data[329], covered by the Council of Europe Convention 108 of 1981, Directive 46/95 /EC and the General Regulation on Data Protection (Regulation 2016/679). This can be seen, among other factors, in the requirement of a legal basis for data processing, in the general principles, in the special rules for sensitive data, and in the fact that the law has as one of its pillars the creation of an authority Protection Policy[330]. Also, clear examples

329 For an analysis of the characteristics of the European data protection model, see: DONEDA, Danilo. From privacy to protection of personal data. Rio de Janeiro: Renovar, 2006; MENDES, Laura Schertel. Privacy, data protection and consumer protection: outlines of a new fundamental right. São Paulo: Saraiva, 2014.

330 EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE. European Court of Human Rights, Handbook on European Data Protection Law, 2014. p. 187 et seq. Available in: <https:/www.fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf>.

of European influence can be perceived, for example, at the rules of responsibility for the operator and controller or in the novelty of data portability, clearly inspired by the European Regulation[331].

In addition, there is an equal and clear influence of Brazilian legislation in the LGPD rules. From the Internet Civil Rights Framework, for example, we have art. 2, which lists the fundamentals of data protection in Brazil. The rule regarding the review of automated decisions evokes the Financial Records Law (Article 5, VI, of Law 12.414/ 2011), a concept previously developed by the European Directive 46/95, but introduced in the Financial Records Law as a right to revision. From the Consumer Defense Code (CDC), there's art. 64 of the LGPD on the dialogue of sources, inspired by art. 7 of the CDC, as well as certain rules of responsibility, in particular the reversal of the burden of proof, exclusions of liability, the possibility of collective damages, as well as the concept of improper treatment of data (article 42, §§ 2 and 3, 43 and 44 of Law 13,709 / 2018). As demonstrated, there are many influences on the LGPD, even supported by the European model of data protection, the LGPD dialogues with Brazilian law and legal culture, and its norms have been influenced by innumerable laws of our legal regime.

In this sense, the Brazilian Law is also the expression of international convergence around basic principles of data protection in the world, a concept that was known from the thesis of Colin Bennett[332]. The author coined convergence of this informally coordinated international phenomenon by which the national legislations were approaching in terms of content and form, in addition to the national peculiarities. Bennett defines convergence as the possibility of identifying, in the dynamics of normative evolution, a pattern in relation to the principles of data protection[333].

331 Ibidem, p. 228.

332 BENNETT, Colin. *Regulating Privacy: data protection and public policy in Europe and the United States*. Ithaca: Cornell University Press, 1992, p. 95 a 115.

333 According to Bennett: "Convergence means more than similarity. It denotes a pattern that goes beyond time, a dynamic process, rather than a static condition. [...] Thus, from a position where States had no or very little data protection legislation and therefore there were several types of strategy for the subject, a consensus emerged during the 1970s, around principles. We can therefore conclude that convergence has occurred. "Ibidem, p. 111 e 112.

17.2 Main axes of LGPD

It is possible to identify five main axes of the LGPD around which the protection of the data data subject is articulated: i) unit and generality of the application of the Law; ii) legitimation for the processing of data (authorizing hypotheses); iii) principles and rights of the data subject; iv) obligations of data processing agents; v) accountability of agents.

The first axis concerns the material scope of the Law, characterized by its generality and unity: the Law focuses on the protection of citizen data, regardless of who performs its treatment, thus applying both to the private and public sectors, irrespective of the data processing modality (Article 3). Its scope of application also covers the processing of data carried out on the Internet, either by its conception of General Law or by express provision of its art. 1 st. These are fundamental features in a general law, which allow the citizen's safety regarding their rights regardless of the modality of data processing and who performs it, as well as provides isonomic treatment among the various entities that treat data, which facilitates their flow and use. It should be noted that only the data referring to natural persons are protected under the LGPD. The few exceptions to the application of the Law are expressed mentioned and are based on the application of a fundamental right (freedom of information, as in the case of the exception to journalistic activity) or relevant public interest (as in exceptions to public security and national defense), under the terms of an article of the LGPD. Such exceptions, however, are shaped in a way that does not compromise the integrity of the Law, and in several of them refer to the existence of specific legislation on data protection that defines the principles of the LGPD.

According to Bennett: "Convergence means more than similarity." It denotes a pattern that goes beyond time, a dynamic process, rather than a static condition. [...] Thus, from a position where States had very little data protection legislation and hence there were several types of strategy for the subject, a consensus emerged during the 1970's around principles.

The requirements for consent to be considered valid by the Law are already foreseen in its definition (Article 5, XII), according

to which consent must be free, informed, unequivocal and for a specific purpose[334]. In the case of treatment of sensitive data, consent must still be provided in a specific and prominent manner, in accordance with art. 11, I, of LGPD. If the consent is formulated only generally or based in misleading information provided to the data subject, the consent will be void, as determined respectively by arts. 8, §§ 4 and 9, paragraph 1 of the Law[335].

Although it is the instrument in which the expression of the will of the data subject classically finds its expression, there are several other hypotheses of treatment of data capable of, also, to legitimize its treatment. Among them, it is worth mentioning the treatment that aims to fulfill the obligation provided for in Law or regulation (article 7, II) or for the performance of a contract of which the data subject is a party, at his request (article 7, V), and public administration, either when the treatment is necessary for the execution of public policy (article 7, III), or in the general exercise of its powers or fulfillment of its legal attributions (article 23).

The hypothesis of treatment for the legitimate interests of the controller or third party (article 7, IX) appears as a kind of general clause, in which a test of proportionality between the interests in the use of personal data, which are the controller or third party, and the rights of the data subject. In that case, it is verified whether the fulfilment of a particular purpose with the processing of personal data, to which the legitimate interest corresponds, has potential effects on the fundamental rights and freedoms of the data subject. If these remain concrete and potentially affected, it must be concluded that legitimate interest should not be considered as a hypothesis that authorizes treatment.

It should also be noted that the law recognizes the protection of credit as an autonomous hypothesis for the treatment of data, including regarding the provisions in the pertinent legislation" in its art. 7, X. This is directly related to the tradition already

334 For a detailed analysis on consent in data protection, see: DONEDA, Danilo. From privacy to protection of personal data, cit. See also: Article 29 Working Party, Guidelines on consent under Regulation 2016/679. Adopted on November 28, 2017 and revised on April 10, 2018. Available in: <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051>.

335 Regarding the possible limitations of consent, see: BIONI, Bruno Ricardo. Protection of Personal Data – The Role and Limits of Consent. Forensic: São Paulo, 2018.

established in Brazilian legislation to specifically provide rules for data protection in the credit sector, notably the Consumer Defense Code and Law 12.414 / 2011 (known as the Financial Records Law). Considering the nature of the activity and the pertinent legislation, the device encourages a systematic reading of the LGPD along with the legislation regarding credit protection, which specificities are part of the regime that will guide the treatment of data in the sector. Thus, specific elements such as the automatic insertion of negative entries (according to the CDC) or the rules foreseen in the registrations of compliance with the Financial Records Law, specific to the credit sector, will continue to be applied and will be complemented by the set of principles and rights of LGPD, strengthening the systemic unity and extending the warranties of the data subject in these situations beyond the sectoral forecasts.

The third axis of the LGPD is composed from the principles and rights of the data subject. The establishment of a series of data protection principles and rights of the data subject by the Law seeks to ensure, on the one hand, a framework of instruments that provide the citizen with the means to effectively control the use of his data by third parties. On the other hand, it confers a systemic unity to the discipline itself for the protection of personal data – which, due to its intrinsic characteristics or to its insertion in a tradition already matured in several other countries, is inserted in our ordering with its own characteristics, which are left perhaps to look more closely at the particularity of the principles and rights related to the matter.

Firstly, attention is drawn to the concern of the legislator in providing for the enunciation of a series of principles in the letter of the Law. This feature takes into account, among other factors, the novelty of the matter and the need to establish the main beacons for its fundamental principles, both as a matter of uniformity and even didactic, when considering the very heavy weight of several principles presented in the Law – take the example of the principle of purpose, which binds the treatment of personal data to the purpose that motivated and justified its collection. The application of this powerful principle results in the realization of some of the ultimate aims of the Law, namely the consideration that the

processing of personal data is inseparable from its purpose and it can always be evaluated, so personal data can never be considered as an object – a mere *res in commercium*.

A number of other principles are still present, which are common to the vast majority of existing data protection laws that are generally based on a common database, originating from the Fair Information Practice Principles (FIPPs) and contained in documents such as Convention 108 of the Council of Europe. These are principles such as free access, security, transparency and quality. The Act also seeks to address contemporary aspects of data protection and to establish a set of principles that reflect new demands, such as establishing the principle of non-discrimination by data processing, addressing the discriminatory potential of data use or automated decision mechanisms that use of personal data, or even the principle of prevention – which in this case is intended to be the basis for the development of measures related to privacy by design (PbD).

It should also be noted that, in addition to the principles literally stated in art. 6 (in number of ten) and others that may be deduced from the text, the caput of the article expressly refers, as a *primus inter pares*, to the principle of good faith. Regarding the protection of personal data, the establishment of good faith as a duty of conduct is of fundamental importance, especially when taking into account the mass nature of various data processing mechanisms and the inherent opacity of these operations. It is therefore relevant to position this principle in the LGPD, to orient broadly the relations between owners and agents of treatment, whether in situations where duties such as transparency are already minimally delineated, or in many other occasions in which the qualification of duties is necessary of conduct.

The fourth strand of the Act lays down obligations for data processing agents, setting not only limits on the processing of data per se, but also providing for a series of procedures that seek to provide greater security and strengthen the guarantees of data subjects. The nature of several of these obligations indicates that the LGPD goes beyond providing instruments for the data subject's defense and protection – in other words, their effects are not only felt at the request of the data subject. Instead, there are a

number of mechanisms that seek to enhance security and prevent problems and damage in data processing. At the same time, there is also the concern to establish a proper system for reparative measures, in case of damage.

Among the main obligations present in the Law, is that of the controller nominate a person in charge of data processing, under the terms of art. 41 of the LGPD. It should be noted that this is an obligation to be fulfilled by the controller and not by the operator. The incumbent will be responsible for receiving complaints from the incumbents, communicating with the national authority and guiding the staff to which the organization complies with data protection standards. The Law itself establishes the possibility of exemption from this obligation, which will depend, however, on a standard to be edited by the National Data Protection Authority (article 41, § 3). The figure of the person in charge, although slightly similar to its counterpart in the GDPR (the Data Protection Officer), does not have the profile of performance delimited in a more comprehensive way as in the European Regulation, although there is provision that the National Authority can also establish new attributions to him.

The LGPD also establishes a central obligation for agents to handle technical, administrative and security measures appropriate to protect personal data from unauthorized access and from accidental or unlawful situations of destruction, loss, alteration, communication or any form of improper or illicit treatment. It is what establishes the art. 46, which opens the information security chapter of the LGPD, applicable to both controllers and operators.

The information security chapter is a fundamental pillar of the Law and brings at least three important innovations to the Brazilian legal system regarding the obligations of treatment agents[336]. First, it requires from everyone dealing with data the adoption of measures that ensure the integrity, confidentiality and availability of the data being processed. Secondly, in the event of a security incident, such as data leakage, an obligation arises for the controller to notify the

336 For the relationship between data protection and consumer protection, see: MENDES, Laura Schertel. Information security, protection of personal data and trust. Journal of Consumer Law, São Paulo, year 22, v. 90, p. 245-261, Nov.-Dec. 2013.

data protection authority, which may determine, as appropriate, the adoption of measures to mitigate the effects of the incident or wide dissemination to society (article 48). Thirdly, there is an obligation in the aforementioned chapter that falls within the concept of Privacy by Design, as it is extracted from art. 46, § 2: "The measures referred to in the main paragraph of this article shall be observed from the conception stage of the product or service until its execution".

A very characteristic obligation is for the controller to conduct a privacy impact assessment, which is a description of a personal data processing operation that is performed together with the measures it has taken to increase security and mitigate the risk present in the treatment. This report shall be requested by the National Data Protection Authority, pursuant to art. 38 of the LGPD.

The fifth axis of the Law is the responsibility of the agents in the event of damages arising from the processing of data and is regulated in section III of Chapter IV.

Consideration of the liability of agents takes into account, firstly, the nature of the data processing activity which the LGPD seeks to restrict to assumptions based on a legal basis (Article 7) and which do not contain more data than is strictly necessary (principle of purpose, Article 6, III) nor are they inadequate or disproportionate in relation to their purpose (Article 6, II).

These limitations to the processing of data, together with the verification that the LGPD takes as a rule the elimination of the data when its treatment is closed (article 16) and also the wave that makes on several occasions the need to take into account the risk present in the treatment of data, indicate that the Law seeks to minimize the chances of treatment to those that are, in a general sense, useful and necessary, and that even these may be limited when verifying the risks to the rights and freedoms of the data subject. It is, therefore, a regulation that has as one of its main principles the reduction of risk, taking into account that the data processing presents intrinsic risk to its owners.

Thus, it is justified that the legislator opts for a regime of strict liability in art. 42, binding the obligation to repair the damage to the exercise of personal data processing activity.

The scheme also lays down specifications as to the liability of certain agents. In this case, the operator will only be liable for acts that it commits that are contrary to the Law or the instructions given to it by the controller, in which case the joint liability regime between controller and operator applies. The controller, therefore, bears responsibility in other cases. Eventually, if there is more than one controller ("joint controllers"), both parties shall be jointly and severally liable to the owner in order to ensure compensation (article 42, § 1, II). These are, in fact, the only two hypotheses of solidarity foreseen in the LGPD, which do not have solidarity as a rule. The Law also provides for the right of return in its art. 42, § 1, IV.

Finally, the Law provides for exclusions of liability in its art. 43, that is to say, where agents prove that they have not processed the personal data assigned to them (I), that although they have processed their personal data, there has been no breach of data protection legislation (II) or that the damage is due to the sole fault of the data subject or third party (III).

17.3 Current Challenges and Possible Solutions

In the act of sanctioning the LGPD, Articles 55 to 59, which dealt with the creation of a National Data Protection Authority (ANPD) and a Data Protection Board, were vetoed. According to the reasons for the veto, the said devices have incurred an initiative vice, violating art. 61, § 1, II, and cumulated with art. 37 of the Constitution. These articles were, utterly modified and re-introduced in a kind of executive decree ('*Medida* Provisoria') by the president of republic in late 2018 and approved by the Congress and enacted as the Law 13.853 of 2019, which modified LGPD creating the Authority and modifying some of its articles.

There is no doubt that the creation of the National Data Protection Authority (ANPD) is a fundamental pillar of the LGPD. After all, the Law gave it such important functions as supervising data processing and sanctioning noncompliance with legislation, regulating hypotheses not specified in the legislation, guiding society about the application of the Law and receiving demands on violations of the rules of protection of data.

An analysis of the more than 40 hypotheses of the legal text in which the Authority is called to act demonstrates that its competence ranges from soliciting and analyzing privacy impact reports, determining measures to reverse the effects of data leaks, to the authorization of the international transfer of personal data. This demonstrates that the agency is not merely a supporter of the data protection system: on the contrary, it is its support pillar, without which the normative and theorecological framework is not able to function adequately.

That is why about 100 countries around the world currently have similar authorities, some of which were created in the early days of personal data protection in the 1970s (such as the German, Swedish and French authorities), and the majority the 1990s and the 2000s, along with the enactment of their national laws, according to the latest census of the International Conference of Data Protection and Privacy Authorities (ICDPPC). Recent data indicate that of the 120 countries that have Data Protection Laws, only 12 did not create an independent authority responsible for their application and because of this they are internationally known as part of a small "corridor of shame" (GREENLEAF, 2017).

In view of profile of the ANPD, which isn't autonomous nor independent as it is located inside the Presidency of republic, it remains clear that the great challenge today for the effectiveness of the Data Protection Law relates to its nature. Without a central, independent and technically credible authority, the consistent and harmonious application of the Law in sectors as diverse as those within its scope is unlikely to be possible. Only through such an authority, with the competence to act and encourage institutional cooperation, will it be possible to overcome the risk of harmonization of multiple and conflicting decisions among the various actors legitimated to act in the protection of personal data, considering the current Brazilian institutional arrangement.

Another important challenge is cultural change, which is necessary for the effective implementation of the Law. After all, the LGPD sets out the principles of necessity and purpose, which indicate that personal data can only be processed when treatment is necessary to meet the needs of the data controller and if its use

occurs within the context or in a manner compatible with the purposes for which the data was collected. That is, a true cultural change is necessary to incorporate the understanding that every personal data is worthy of legal protection, since it is a means of representing the person in society.

Finally, there is the challenge of systematically interpreting the various laws regarding the processing of personal data in Brazil, in particular, the LGPD with other laws that deal with specific sectors, such as the Internet Civil Registry and the Positive Registration Law. The challenge is particularly important insofar as the classical solutions of conflict of laws in time – whether relating to the specialty of one of the standards or the derogation from the earlier Law – do not appear to be appropriate in this case. One solution to this dilemma lies in the application of the dialogue of the sources, developed by Claudia Lima Marques in the wake of the teachings of Erik Jayme. As explained by Claudia Lima Marques, the dialogue of the sources is "the current simultaneous, coherent and coordinated application of the plural sources of legislation, special laws (such as CDC, Health Insurance Law) and general laws (such as CC / 2002), with convergent but not more equal fields of application" .

17.4 Conclusion

The subject of data protection has become a key component for the protection of the citizen, the consumer and the very security of society in a hyperconnected world in which personal data is the input of countless economic activities in the online world and off-line, and are also essential for the public sector[337]. It is sufficient to think of the flow of credit and financial data to analyze the consumers 'payment capacity, data about patients' health, behavior and habits collected on the internet, among others, which demonstrates the ubiquity of computing means (ubiquitous computing[338]), as well as data processing.

337 VESTING, Thomas. § 20 Die Bedeutung von Information und Kommunikation für die verwaltungsrechtliche Systembildung. In: HOFFMANN-RIEM, Wolfgang et al. *Grundlagen des Verwaltungsrecht, Band II.* München: Beck, 2008. p. 22.

338 MATTERN, Friedemann. Allgegenwärtige Datenverarbeitung – Trends, Visionen, Auswirkungen... In: ROßNAGEL, Alexander et al. *Digitale Visionen:* Zur Gestaltung allgegenwärtiger Informationstechnologien. Berlin: Springer, 2008. See also: HARTMANN, Maren; WIMMER, Jeffrey. Einleitung. In: HARTMANN, Maren; WIMMER, Jeffrey. *Digitale Medientechnologien: Vergangenheit – Gegenwart – Zukunft.* Wiesbaden: VS, 2011. p. 21.

The legitimate and responsible use of personal data provides the citizen with the confidence to make the better use of its own data whenever he or she deems appropriate, as well as guarantees legal certainty treatment agents so that they can use them transparently in their business models. To achieve this end, a system of standards for data protection have been developed, which involves establishing a series of procedures, principles and rights that limit the processing of personal data while empowering the citizen to control the flow of their data. In this sense, the sanction of the LGPD was certainly a huge advance in the Brazilian regulatory framework.

However, its effective implementation depends on the constitution of a personal data protection authority, supported by a tripod that is consistent with sanctioning power, expertise and independence. Without building this regulatory architecture, it will not be possible to achieve its main objective, which is to consolidate the trust of society in the information and communication infrastructure, guaranteeing rights, expanding innovation and providing greater competitiveness between services that use in a legitimate way personal data. The effective application of the LGPD will also depend on a cultural change that understands that all personal data is worthy of legal protection. Furthermore, it is essential to consolidate a systematic interpretation of the LGPD with the other normative diplomas that deal with the processing of personal data, along the lines of the dialogue of the sources, enabling the simultaneous application of the general principles and rules of the LGPD with the sector rules[339].

Finally, it should be emphasized that the discipline of personal data protection concerns a subject in constant evolution and that the Brazilian legal system must pay attention to the technological developments that daily change the life of the citizens, the forms of work, the cities and the economy in contemporary society. These changes also influence the development of data protection issues. Significant evidence of new developments in

339 As Alexandre Veronose and Noemy Melo point out, such a dialogue will also have to be made among the norms that regulate the activities of the telecommunications, media and information technology sectors. (In Portuguese), in the context of the new European Law (2016/679 EU)., pp. 71-99, Jan.-Mar. 2018.

this area has been the review by the OECD of the Guidelines for the protection of personal data and the cross-border data flow of 2013[340], the edition of the European Data Protection Regulation in 2016, which entered into force on May 25, 2018, as well as the recently approved California Data Protection Act [341]. In addition to these changes at the institutional level, the transformation of the concept of privacy and data protection can also be seen in information theory, as Helen Nissenbaum's work demonstrates. The author advocates for a more complex and broader concept of privacy than the definitions hitherto known, which focus used to be the control of the individual over his or her personal information or the preservation of intimate and private events[342].

From the foregoing, it can be seen that LGPD was an important step towards strengthening the normative framework of the information society in Brazil. It is now necessary to develop a data protection culture, to build a solid institutional framework for the implementation of the LGPD, as well as an in-depth doctrine on the different issues addressed by the Law, providing legal certainty for the actors in the digital economy, protecting the data subject's confidence and encouraging the country's economic development in this area[343].

340 These guidelines, which constituted the first international agreement on the subject and were issued in 1980, were reviewed for the first time in 2013. Available in: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

341 California Consumer Privacy Act of 2018, Disponível em: <https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375>.

342 Nissenbaum defines privacy as "contextual integrity", stating that privacy is not a right to secrecy, nor a right to control, but rather the appropriate flow of personal information, according to informational norms oriented by social contexts informational norms). Violation of privacy will then occur whenever such information standards are disobeyed. The verification of privacy violation under this perspective requires the analysis of a series of criteria, such as contexts (structured social environments), actors (emitters, receivers and subjects of information), attributes (types of information) and transmission principles (confidentiality, reciprocity, necessity, etc.). In addition, it states that in some cases a broader assessment is required of the risks caused by the flow of information to the autonomy and freedom of the individual, as well as to equality, justice and democracy. (NISSENBAUM, Helen, "Privacy in context: technology, policy, and the integrity of social life." Stanford: Stanford Law Books, 2010.)

343 See study on the importance of digital trust for organizations in: <https://www.ca.com/us/collateral/white-papers/the-global-state-of-online-digital-trust.html>.

17.5 References

Article 29 Working Party. *Guidelines on consent under Regulation 2016/679*. Adotado em 28 de novembro de 2017 e revisado em 10 April 2018. Disponível em: <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051>.

Benjamin, A H, Marques, C L & Bessa L (2008). *Manual de Direito do Consumidor.* São Paulo: Ed. RT.

Bennett C (1992). Regulating Privacy: data protection and public policy in Europe and the United States. Ithaca, New York: Cornell University.

Bioni, B R (2016). Autodeterminação informacional: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. Universidade de São Paulo, São Paulo.

Doneda D (2006). *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar.

Doneda D & Mendes L S (2014). Data Protection in Brazil: New developments and current challenges. In: GURWIRTH, S.; LEENES, R. DE HERT, P. (Org.). *Reloading data protection*: multidisciplinary insights and contemporary challenges. Berlin: Springer.

Greenleaf G (2017). Data Privacy Authorities (DPAs) 2017: Growing Significance of Global Networks. In: *Privacy Laws & Business International Report*, 146, março 2017, p. 14-17.

Hartmann M & Wimmer J (2011). Einleitung. In: Hartmann M & Wimmer J. *Digitale Medientechnologien: Vergangenheit – Gegenwart – Zukunft.* Wiesbaden: VS.

Mendes L S (2013). Segurança da informação, proteção de dados pessoais e confiança. *Revista de Direito do Consumidor*, São Paulo, ano 22, v. 90, p. 245-261, nov.-dez.

Mendes L S (2014). *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva.

Marques C L (2012). O "diálogo das fontes" como método da nova teoria geral do direito: um tributo à Erik Jayme. In: MARQUES, Claudia Lima (Coord.). *Di*álogo das Fontes: do conflito à coordenação de normas do direito brasileiro. São Paulo: Ed. RT.

Mattern F (2008). Allgegenwärtige Datenverarbeitung – Trends, Visionen, Auswirkungen... In: ROßNAGEL, Alexander et al. *Digitale Visionen*: Zur Gestaltung allgegenwärtiger Informationstechnologien. Berlin: Springer.

Nissenbaum H (2010). *Privacy in context*: technology, policy, and the integrity of social life. Stanford: Stanford Law Books.

U.S. Department of Health, Education and Welfare (1973). *Records, Computers and the Rights of Citizens*. Disponível em: <https://aspe.hhs.gov/report/records-computers-and-rights-citizens>.

Veronese A & Melo N (2018). O Projeto de Lei 5.276/2016 em contraste com o novo Regulamento Europeu (2016/679 UE). *Revista de Direito Civil Contemporâneo*. São Paulo: Ed. RT, v. 14, ano 5, p. 71-99, jan.-mar. 2018.

Vesting T (2008). § 20 Die Bedeutung von Information und Kommunikation für die verwaltungsrechtliche Systembildung. In: HOFFMANN-RIEM, Wolfgang et al. *Grundlagen des Verwaltungsrecht, Band II.* München: Beck.

18 Privacy, Personal Data and Tensions with Freedom of Expression On-line

Eduardo Molina Quiroga

Abstract

The right to privacy, or private life, which appears as protectable at the end of the 19th century and is recognized in the Human Rights Treaties in the second half of the 20th century, is related to the right to the protection of personal data, without prejudice to the conceptual autonomy that this is reaching in the last triennium of the last century. Both suffer a remarkable change with the dissemination of ICTs and especially the Internet. The conflict unleashed in this scenario confronts these rights with other freedoms, such as freedom of expression. The present work tries to describe the main characteristics of the aforementioned rights and present a proposal of criteria to take into account when resolving these conflicts.

18.1 Introduction

The recognition of the so-called right to privacy as a good subject of legal protection seems to date back to the late nineteenth century, since until then it was considered exclusively as a fact resulting from social custom or the so-called moral respect due to the person. In 1980, Samuel D. Warren and Luis D. Brandeis published a work entitled "The Right to Privacy" in the Harvard Law Review[344], where they stated that every individual has the right to "be left alone" or "not to be disturbed", that is, the need to acknowledge the existence of an intimate life, which should be protected in an equivalent way to private property. It is also mentioned that Kohler, in Germany, had already referred in 1880 to an "individual right that protects the secret of the intimate life of unauthorized advertising"[345]. The American Judge Thomas A.

344 See Warren & Brandeis (1890).

345 Quoted by Fernández Sessarego (1992).

Cooley, in his work *The elements of Torts*[346] seems to be tha one who defined "intimacy" as "*the right to be left alone*", concept that the doctrine traditionally understands in as "the right to be left in peace", or "the right to be left alone".

It has been argued that the development of the concept of the right to privacy and private life, within the liberal ideological framework, is presented as a right to freedom, as the right of the individual to do what he / she feels, that is, to be alone, not to be bothered, to make decisions in the private sphere without external intervention. This non-interference includes, among others, decisions regarding sexual freedom, the freedom to act freely within one's home, the freedom to reveal or not intimate behaviors and freedom to identity. These concepts were developed at the end of the 18th century in the heat of an ideological movement in which the State was seen as an "enemy". The concept of freedom has sense of negative liberty, which implies not suffering interference from others (a passive right), and the broader the area of non-interference, the broader the freedom. Even when it is admitted that the free action of men must be limited by law, a minimum area of personal freedom must be preserved that must not be violated, in order to preserve the minimum development of the natural faculties. This explains the need to draw a border between the area of private life and that of public authority.

The salient feature of this "right to privacy," according to the original description by Warren and Brandeis, was that it was not a right recognized by the individual against the public power of the state, but a right recognized to individuals in front of other private individuals substantially conformed by means of the press through which the "invasion of privacy" took place. It was an individual right of an infraconstitutional nature, the breach of which by another particular and substantially by the press, gave the right to claim damages (the "damages") whose existence could only be considered as such, since it had not mediated a" consent "to the publication.

The expansion of the right to privacy concept from the private law scope to its interpretation as a subjective right of constitutional

346 See Cooley (1895).

nature, did not occur until the end of the Second World War. The question was explicitly considered by the US Supreme Court when it resolved in 1967 the previous "Katz"[347], where he pointed out that the fourth Amendment of the American Constitution, regarding the inviolability of the domicile, should be interpreted as to "protect people and not places", which configured a substantial expansion of the right to privacy, from the private law sphere towards a larger universe, in which a "protected constitutional area" of individual intimacy took root.

18.2 Concept

Apprehending the notion of privacy is not a simple issue because of the multiplicity of definitions or descriptions that the doctrine has made on this subjective right. It is also called the right to privacy. The doctrine has conceived the right to privacy in various ways, some wider and more in line with the technological evolution of our days and others more restricted.

The right to privacy has been evolving in its conception, in line with the technological changes that have occurred in humanity, in such a way that its initial conception of restricting the access of third parties to a certain part of people's lives, a negative position, not doing on the part of society, has changed by the current conception that, basically, includes the right to control the information that in relation to a person exists in the media[348]. The modern conception of the right to privacy has an intimate relationship with the technological developments that have made it possible to collect data, which belongs to the private sphere of people, in the different activities of current economic life.

347 See Katz vs. United States; 389 US 347,351 (1967).

348 Particularly in the European Union, the Charter of Fundamental Rights distinguishes "respect for private and family life" (art. 7) and the "protection of personal data" (art. 8.) Respect for private and family life \ > Everyone has the right to respect for his or her private and family life, home and communications. Article 7. Article 8 Protection of personal data 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority. It is also worth mentioning the constitutions of Portugal (art. 35); Hungary (art. 59); Finland (art. 10); Slovenia (art. 38); Slovakia (art. 19); Poland (art. Among others. In a less express way should also be cited art. 18 of the Spanish Constitution.

In relation to the so-called "secrets", the right to privacy is also considered as one of the foundations of the secret to communications, which currently, with technological development, has made this concept expand enabling the violation of any communication, among which stand out digital telephony, mobile telephony, emails, Internet exchanges, among others.

A fundamental issue that results from technology, in terms of privacy, is the so-called "data banks" that are formed in both public and private institutions, and even in offices of professionals, through the exercise of their daily activities. The right to privacy has a very close relationship with freedom of expression and freedom of the press, in fact, as we indicated in the background, this right arises as a result of the meddling of the written press in the most personal spheres of people. This relationship was made explicit in the context of the Argentine constitutional reform of 1994, which established, in article 43, a third paragraph that reads: "Any person may bring this action to take cognizance of the data referred to and its purpose, that they appear in registers or public data banks, or the private ones destined to provide reports, and in case of falsehood or discrimination, to demand the suppression, rectification, confidentiality or update of whom the secret nature of the sources of journalistic information shall not be impaired". In this way, the protection of personal data was introduced in our Brazilian Federal Constitution.

Although there is no consensus on this, it is considered that "private life" is gender and includes intimacy as a central core, although they can be used as synonyms. Regarding the notions of "reservation" and "secrecy", there is a difference of degree: secret would be what is not intended to be known by third parties, while reserved would be that whose public dissemination should be avoided. The explanatory statement of the repealed Spanish LORTAD 5/92 clarifies that

> "[...] there is talk of privacy and not of intimacy: it is broader than this, because as privacy protects the sphere in which the most singularly reserved facets of the person's life develop – the address where he performs his daily life, the communications in which

> he expresses his feelings, for example – privacy constitutes a broader, more global set of facets of his personality that, isolated in isolation, may lack intrinsic significance but, coherently linked to each other, they throw as a precipitate a portrait of the personality of the individual that he has the right to keep reserved and if intimacy, in the strict sense, is sufficiently protected by the provisions of the first three paragraphs of Article 18 of the Constitution (Spanish) and by the laws who develop it, privacy can be undermined by the use of computer technologies so recent I develop."

18.3 Regulatory recognition

From the point of view of the normative antecedents referred to the protection of the right to privacy, numerous treaties and international declarations can be cited, which consecrate the fundamental range of such right, such as the Universal Declaration of the Rights of Man of the Assembly General of the United Nations (1948); the American Declaration of the Rights and Duties of Man (1948); the European Convention on the Safeguarding of Human Rights and Fundamental Freedoms (1950); the American Convention on Human Rights (1969) and the International Covenant on Civil and Political Rights (1966); the Charter of Fundamental Rights of the European Union (2000). Mention should also be made of the Convention on the Rights of the Child (1989), the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (1990), among other international instruments.

In Argentine law, we can cite article 19 of the National Constitution, which enshrines the so-called "reserve principle", article 18, which guarantees the inviolability of domicile, correspondence and private papers, and article 33 which recognizes So-called "implicit rights". We also mentioned the old Law of trademarks (art. 4 law 3975), as well as the provisions of law 11,723 of intellectual property (arts. 31 and 32), art. 1071 bis of the repealed Civil Code (Law 21,173), and the arts. 51 and following in Civil and Commercial Code. In the judicial

field, the Argentine leading case was Ponzetti of Balbín, in which the Supreme Court of Justice of the Nation held that

> "The right to privacy and privacy is constitutionally based on art. 19 of the supreme law."... article 19 affords legal protection of an area of individual autonomy that comprises feelings, habits and customs, family relations, economic status, religious beliefs, mental and physical health and, more generally, the activities, acts or information which, having regard for the way of life accepted by the community, are confined to the individual, so that knowledge or disclosure of them by other persons would represent a real or potential danger to privacy.

This single ruling proposes that

> "The right to privacy includes not only the domestic sphere, the family circle of friendship, but other aspects of people's physical spiritual personality, such as bodily integrity or image, and no one can interfere in a person's private life, their consent, or their authorized relatives, and only by law can interference be justified, provided there is a greater interest in safeguarding the freedom of others, the defense of society, manners or pursuit of crime".

18.4 Concept of personal data

The data by themselves do not allow us to adopt the most convenient decision because they do not provide the necessary knowledge. We must add, combine, exclude, and compare, these data to obtain a result that is useful to us. It is what we call data processing. The "information" is the result of this transformation (processing) of the data.

The recorded data may belong to a person or a thing, or to the relationship of both. When the segment of reality that is the object of information is a person, identified or identifiable, we are dealing with personal data, with a broad scope, that is to say that if possible treatment operations can establish relationships, references or associations, with people – whether determined or determinable –

the data involved must be considered as "personal data", and must be taken into account[349].

Within the genre "personal data" are called "sensitive" (or require special treatment)[350] those referred to certain facets or aspects of a person, such as the cult he professes, his racial belonging, his political ideology, his sexual behavior, and in general the information that allows him to determine his moral and ideological appearance. The essential concern surrounding the treatment of these data, in addition to the protection of the right to privacy, or private life, is without doubt, the possibility of discrimination, expressly mentioned in art. 43 of the Argentine Constitution.

18.5 Impact of new technologies

The eruption of information technology forced a rethinking of the right to privacy, the structuring of large personal data banks, and the possibility of cross-linking the information contained therein. With the spread of the computer phenomenon begins to speak of "protection of personal data."

Therefore, we have argued that the right to privacy can no longer be considered simply the absence of information about us in the minds of others (the "leave me alone"), but it is overcome and acquires the character of a control over information that concerns us, that is, the faculty of the subject to control the personal information that will appear in the data banks.

The right to "data protection" belongs to the context of the computer age, and it is increasingly doubtful to affirm that this complex legal discipline is already implicit in the general references to the right to privacy, inserted in normative bodies of the national scope or international of the pre-computing era.

18.6 Informative self-determination

The legal basis of the right to the protection of personal data must be related to the traditional right to privacy, or to private life, but

349 For example, the host 2 subsection a) Law 25.326 (Argentine Personal Data Protection Law).

350 For example, arts. 2 inc. b) and 7 and conc. Argentine Law 25,326.

it exceeds it to a great extent. The control of personal information is linked to the concept of individual autonomy to decide, up to a certain limit, when and what information referred to a person, can be subject to automated processing, so it has also been called the protection of personal data, informative self-determination, and even computer freedom.

The central point of this evolution – from protection to privacy towards the recognition of an autonomous right – is found in the jurisprudence of the German Constitutional Court.

In a first stage, the German jurisprudence had supported the call "theory of the spheres", according to which a Differentiated protection according to the greater or lesser degree of affectation of privacy[351].

This restrictive conception was abandoned in favor of a considerably broader protection, in the ruling known as the "census decision"[352], in which the German Constitutional Court was issued in relation to a Census Law, voted by the Parliament (Bundestag), according to which, in order to improve the use of social resources, citizens were compelled to answer an interrogation that covered a series of private data. Although the data were collected anonymously, they were to be compared with those registered in the Federal States (Länder), and this, hypothetically, would allow identifying their owners. The Court, although it confirmed the validity of most of the law, was forced to make modifications in certain points, relating to the way in which data collection and storage could be authorized[353].

351 This doctrine was elaborated especially in the case about the Mikrozensus, cf. BVerfGE 27, 1 and following; Alexy, Robert, "Theorie der Grundrechte", 1994 (second edition), p. 327 translated by Garzón Valdés, Ernesto as "Theory of fundamental rights" (Center for Constitutional Studies, Madrid, 2002 (3rd, reprint), p.349 et seq.; Alexy, Robert, "Fundamental Rights in the Democratic Constitutional State," in Carbonell, Miguel (Edit.), Neo-Constitutionalism (s), 2nd Edition, Trotta, Madrid, 2005. See adde: Hassemer, Winfred and Sánchez, Alfredo Chirino, "The right to informational self-determination and the challenges of automated processing of personal data", Editores del Puerto, Buenos Aires, 1997, p. 172.

352 Judgment of 12/15/1983 (Ref. 1 BvR 209/83) in the unconstitutionality lawsuits against the Law on the recount of the population, professions, housing and work centers (1983 Census Law) of 03/25/1982 (published in the Federal Legislation Bulletin -BGBI- I, p. 369), the Federal Constitutional Court – First Chamber – issued said judgment, with the participation of President Benda and Judges Simon, Hesse, Katzenstein, Niemeyer, Heussner, Niedermaier, Henschel (according to extract published by the magazine Contemporary Public Law No. 7), of the Lawyers Association of the General Comptroller of the Republic of Colombia, based on some parts of the sentence translated by Manuel Daranas, for the Bulletin of Constitutional Jurisprudence No. 33, of 1984).

353 See recession in Kommers, Donald, "The Constitutional Jurisprudence of the Federal Republic of Germany," Durham, London, 1989, p. 332 and vote Dr. Petracchi in "Urteaga".

The protection of personal data does not arise exclusively as a result of individual problems, but also expresses conflicts that include all individuals in the international community, a problem that is analyzed from the perspective of the international flow of data. This right not only includes an individualistic idea of privacy protection but also protects the interests of a social group against the processing, storage and collection of information, especially if we notice the link with discriminatory practices.

The automated processing of personal data has become a strategic weapon for manipulating individual behaviors[354], and the application of advanced telematic methods to personal information has ceased to be the exception to become a daily routine.

The right to protection of personal data, related to the traditional right to privacy, exceeds it because it reaches data that is public, or if you want, non-confidential, and affects other personal rights such as honor, image, or the identity. It is a concept that gradually acquired the recognition of an individual right of very personal character[355], both in the doctrine and in the legislation.

The core of the protection of personal data is directed to a person having the possibility of controlling the veracity of the information and its use[356]. The lordship of man over himself extends to the data about his habits and customs, his system of values and beliefs, his patrimony, his family, economic and social relations, with respect to all of which he has the right to self-determination[357].

354 Cf., among others: Correa, Carlos and others, "Computer, Freedom and Human Rights", in Correa, Nazar Espeche, Czar de Zalduendo and Batto, "Computer Law", Depalma, Buenos Aires, 1987; Giannatonio, Ettore, "Introduzione all'informatica guiridica" cited in: "Impact of Information Technology in society" (Protection of personal data. Right to privacy); Stiglitz, Rosana M., LA LEY, 1987-E-859; Carrascosa López, Valentín, in "Right to Privacy and Information Technology", in Informatics and Law UNED, 1-1992, pag. 23, etc.

355 They are considered "very personal rights or" personality rights ", the recognition of the right to life, freedom, aspects related to honor, etc., which have been included in local laws (for example, arts. 52 and conc.Civil Code and Argentine Commercial), but also by the impulse of the universal doctrine that provoked, especially after the World Wars, a systematic consecration, in international norms such as the Universal Declaration of Human Rights (1948) or the Pact of San José de Costa Rica (1969), and they have also been consecrated in numerous Constitutions.

356 See for a critical perspective on the efficiency of informational self-determination, see Belli, Schwartz and Louzada (2017).

357 Supreme Court of Justice of the Nation, 15/10/1998, "Urteaga, Facundo R. c / Joint Staff of the Armed Forces", vote of Dr. Santiago E. Petracchi, LA LEY, 1998-F, 237.

18.7 Internet

Internet access has become a powerful tool for socializing knowledge and promoting communication between individuals and social groups. The large amount of information stored on the network would not have the current effects if it did not have an effective communication system. This mode of communication and access to information has become a true new pattern of forms of interrelation. Like all technology, the Internet is a cultural creation that reflects the principles and values of its inventors, who were also its first users and experimenters. The libertarian values of those who created and developed the Internet determined an open architecture that was difficult to control.

At the same time, when society realized the extraordinary capacity represented by the network, the values embodied in it were disseminated throughout the social life, particularly among the younger generations. For a sector of opinion, to which we adhere, the Internet and freedom have become synonyms throughout the world. This does not exclude that other sectors see the Internet as an area in which rights violations occur. However, we subscribe to the opinion it holds, such as the Office of the Rapporteur for Freedom of Expression of the Organization of American States "that freedom of expression applies to the Internet in the same way as to all media" and added that "States have an obligation to promote universal access to the Internet to guarantee the effective enjoyment of the right to freedom of expression. Access to the Internet is also necessary to ensure respect for other rights, such as the right to education, health care and work, the right of assembly and association, and the right to free elections"[358].

It is not strange to link the expressions of land use, interconnectivity, accessibility, heterogeneity of contents, when the establishment of limitations or restrictions is sought, in order to avoid conducts that controvert social order through the Internet. Since the Internet is an open or public network, it has the characteristic that no one can be prevented from accessing it. The Internet network currently

358 "Joint Declaration on Freedom of Expression and the Internet", June 1, 2011, points 1.a and 6.a, respectively as cited by CSJN, 10/28/2014, Rodriguez, Maria Belen vs. Google and other s / damages. R. 522. ILL.

allows the exchange of data between the five continents, enabling access to all kinds of content as well as its transmission, between any users of the world connected to the network, which has led to say that it is "landed".

Currently one of the phenomena that has generated more controversy is the eventual responsibility for the contents published on the network, especially that are attributed to the so-called "seekers", dividing judicial decisions and doctrinal opinions among those who understand that suppliers of the different services, such as access to the network, accommodation (*hosting*), content and search engines, in principle are not responsible, a position that predominates in comparative law, and who, on the contrary, understand that they can impute the consequences of such content. In this current manner, positions bifurcate between those who understand that the attribution factor is subjective (fault or fraud) and the defenders of strict liability, either by location or risk created[359]. In general, legislation is very scarce, a situation that is difficult to reverse, insofar as the network is a global phenomenon with universal access and general reach, which until now has eluded all or almost all attempts at state control.

The problem that arises when it comes to legislating on the matter is that the Internet advances very quickly, and when a law is passed, it is very possible that the technology has changed. For this reason, the interpretative role of the judge is noteworthy, based on the principle of analogy and the "reasonableness standard". A balance of the rights at stake must be established, combining them with the public interest (a weighting judgment) privileging the highest hierarchy or – in the same range – the one with the highest axiological content, in the line of the most equitable solution, as a result less burdensome to the general interest, and fairer according to the particularities of fact. Reasonableness – which is not at odds with the logic in the decision making by the magistrate – must

359 To expand see Molina Quiroga, Eduardo, "Responsibility of the searchers. Analysis of the subject in the light of comparative law and the jurisprudence of the Supreme Court of Justice ", The Online Law; Magazine Civil and Commercial Code (Special Edition) The Law, October 2015, III, 173/182. Online Appointment**:** AR / DOC / 2974/2015; Molina Quiroga, Eduardo, "Social networks, personal rights and freedom of expression", LAW 16/08/2017, 5, AR / DOC / 2149/2017; Idem, "The right to image and the responsibility of search engines. A new sentence of the Court ", THE LAW 03/10/2017, 4, AR / DOC / 2535/2017, among others.

preside over all judicial decisions. In our opinion, it is imperative to reformulate the criteria and guidelines with which it is proposed to make predictable behaviors on the network, and above all, to provide effective responses that the law must provide when legitimate interests are affected, often in conflict.

18.8 Tensions between freedom of expression and data protection

Under the guarantee of "freedom of expression", the freedom to express an opinion and the right to give or receive information or ideas, without prior censorship or without interference by authorities, are universally understood. It is considered as one of the fundamental guarantees of democratic societies, and any person can claim to be respected the exercise of this guarantee. Thus, the Universal Declaration of Human Rights (art. International Covenant on Civil and Political Rights. 19); Rome Convention of 1950 (art. 10); Charter of Fundamental Rights of the European Union of Strasbourg, 2007 (art. eleven); American Declaration of the Rights and Duties of Men, Bogotá, 1948; American Convention on Human Rights (art. 13); African Charter on Human and Peoples' Rights, Nairobi, 1981 (art. Convention on the Rights of the Child 13). Also in constitutions such as Spain (art. 20), among others.

In turn, freedom of the press is linked to freedom of expression in a half-to-end relationship. This relationship can be summarized by saying that it involves expressing what one thinks (which modernly means searching, receiving and disseminating ideas or opinions on any subject) by any audiovisual means. In Argentina, the Supreme Court of Justice of the Nation held that "freedom of expression", in a broad sense, is the substantial right to give / receive information that assists all individuals as "inhabitants" of a democratic state[360]; and defines "freedom of the press", also in a broad sense, as an instrumental right, being the means to satisfy that social need[361]. In a similar line, we must bear in mind the Advisory Opinion of the Inter-American Court of Human Rights that emphasizes that freedom of expression has a "double dimension": individual and

360 CS, 11/9/1991, "Vago, Jorge A.", Judgment 314: 1517.

361 CS, 03/12/1987, "Costa, Héctor R.", Judgment 310: 508.

social, including in the latter the means of social communication that serve to "materialize" the exercise of the first, and that both must be guaranteed simultaneously[362]. In Argentine law, the support of freedom of the press and of expression is fundamentally contemplated by arts 1, 14, 19, 32 and 33 of the Const. National, and by the international instruments with constitutional hierarchy incorporated by the 1994 reform (art. 75, inc. 22), to which we have already referred, and specifically by law 26,032.

Even when all the international and domestic norms of the States recognize and consecrate the guarantee of freedom of expression, it is a right subject to restrictions, generally based on reasons of public order, such as the granting of broadcasting licenses administered by the government. Relevant authority, or whose exercise may give rise to responsibilities arising from its misuse, such as when, during the exercise of freedom of expression, it violates other rights such as honor, privacy of individuals or protection of personal data, incitement or exaltation of racial hatred or the practice of discrimination. In this sense, the International Convention against all forms of racial discrimination in its art. 4º provides for restrictions, as does the Convention for the Prevention and Punishment of the Crime of Genocide (art. III.

The Federal Court of the United States, in the well-known "Reno" case, said that the Internet network can be seen as a global conversation without barriers, so the government cannot interrupt this conversation through any means and that as is the in a more participative form of mass discourses that have been developed, the Internet deserves the greatest protection against any government interference"[363].

18.9 The tension between fundamental rights *on-line*

Regarding the issue of the dissemination or distribution of information of illegal content, each of the States in which the

362 IACHR, 11/13/1985, "The Compulsory Association of Journalists (At the request of the Government of Costa Rica)", Advisory Opinion 5/85, numeral 29 et seq.

363 CS USA, 06/26/1997, "Janet Reno, Attorney General of the United States of America, et al, appellants c / American Civil Liberties Union, et al No. 96-511, elDial AA1748 (full text in Spanish) (1997 US LEXIS 4037).

respective servers are installed may apply its internal legislation, but encounters the difficulty of having no jurisdiction beyond its territorial limits, except in exceptional cases, as for example in matters of genocide and crimes against human rights.

Of course repression is not the same as censorship. The message is communicated, the consequences come later. So, rather than blocking the Internet, what may correspond is that it represses or punishes those who abuse it, according to government criteria. For this reason, it has been argued that both those who declare the Internet uncontrollable and those who consider it the most sophisticated control instrument are right, in the last case under the aegis of the constituted powers. Technically, the Internet is an architecture of freedom. Socially, its users can be repressed and monitored through the Internet. But, for this, the censors have to identify the transgressors, which implies the definition of the transgression and the existence of effective surveillance techniques. The definition of the transgression depends, of course, on the legal and political systems of each jurisdiction.

This is an everlasting debate in which personal dreams, the degrees of (de) technological knowledge, the routine of power, and the speed of change of reference parameters are mixed.

In principle, the design of the network, from a structure in layers, with distributed communication capacity for each node and packet-switched transmission (*packet switching*, in English) operated by TCP / IP protocols, according to multiple alternative communication channels, provides great freedom to the information flows circulating on the Internet.

It has been said that Internet streams interpret censorship (or interception) as a technical failure and automatically find a different route of message transmission. Being a global network with multimodal communication and information processing power, the Internet does not distinguish borders and establishes unrestricted communication between all its nodes.

The only possible direct censorship of the Internet is not to be on the network. Any network connection of computers with Internet protocols allows global communication with any point

of the network. However, if the network is global, access is local through a server. And it is at this point of contact between each computer and the global network that the most direct control occurs. It is possible, and is done in all countries, to deny access to the server, to close the server or to control who communicates what and to whom, by means of an electronic surveillance of the messages that circulate through the server.

And this is increasingly expensive for governments, societies, companies and individuals. You cannot be "a little" on the Internet. There is, yes, the possibility of issuing unidirectional messages propagated on the Internet, without reciprocal communication, to the extent that the servers of a country remain disconnected from the internal network. However, if the network is global, access is local, through a server. And it is at this point of contact between each computer and the global network that the most direct control occurs.

In this context, it is important that there is adequate legal protection of freedom of expression and communication on the Internet.

With regard to the tensions between the freedom of expression on the Internet and the technical viability of controlling the contents circulating on the Internet, we believe that, in reality, the most important thing is not technology, but the ability of citizens to assert their right to the free expression and privacy of the communication, since, in last term, it is in the conscience of the citizens and in its capacity of influence on the institutions of the society, through means of communication and of the own Internet, where the faithful balance lies between the network in freedom and freedom in the network. In a convergent sense, Antonio Martino has said that

> "*All right is already on the Internet. What you have to do is build a standard so that it can be visualized anywhere; what needs to be created is a culture of trust based on knowledge and Knowledge is born from training. Report all measures that affect the free movement of goods, ideas and people by creating this novo ius Gentium*[364]".

364 Martino Antonio, "E-Comerce and Law today. The experience of the European Community ", Ecomder 2000 <http://ecomder.com.ar>.

Regarding the equalization of the Internet to a communication medium, we understand that the new digital technologies of information and communication pose new challenges when it comes to "constitutionalizing" fundamental rights, such as freedom of expression, the right to privacy and the so-called informative self-determination (protection of personal data) and that, in this sense, the expression of law 26.032 "dissemination of information of all kinds" through the Internet must be interpreted in harmony with the protection of these last two rights, the privacy and information self-determination, and it is the judges' task that the synthesis is carried out from a perspective *pro homine*

With regard to search engines, it should not be forgotten that they are now, in short, the central technical mechanism through which people meet on the Internet their right to seek and receive information. From this perspective, the search engines have the ability to enhance the "social dimension" of freedom of expression, in the terms that the Inter-American Court of Human Rights has expressed, insofar as they allow "to receive information and to know the expression of thought alien "that is available on the internet. As the IACHR has observed, freedom of expression has an individual dimension and a social dimension, since "this requires, on the one hand, that no one be arbitrarily prejudiced or prevented from expressing his or her own thoughts and, therefore, represents a right of each person; but it also implies, on the other hand, a collective right to receive any information and to know the expression of the thoughts of others". This social dimension of freedom of expression cannot be underestimated, given that "knowledge of the opinion of others or of the information available to others is as important to the ordinary citizen as the right to disseminate one's own"[365].

Anonymity in the digital domain is one of the guarantees for the establishment of a robust democratic discussion. The Internet allows citizens to express their opinions without fear of reprisals. Therefore, implementing mechanisms that require the delivery of personal data as a condition to be able to issue an opinion

365 I / A Court HR, "Compulsory registration of journalists (arts. 13 and 29, American Convention on Human Rights), "advisory opinion OC-5/85 of 11/13/1985, Series A, no. 5, para. 30).

constitutes a threat to the rights of citizens and is a way to promote the censorship of expressions contrary to the political powers.

Cando is a tension or conflict between the guarantee of freedom of expression and the right to privacy, which will vary is the threshold of protection recognized by the legal system to the person affected, depending on its public or private nature. Consequently, this special constitutional protection determines that, if the basis of a precautionary measure is invoked, for example, the injury to privacy, honor or good name through electronic means, the burden of proof on that point falls on who intends the precautionary restriction.

18.10 Conclusions

Therefore, we understand that when there is a conflict between the very personal rights to honor, name and intimacy of the actor or information self-determination and those that protect the freedom of expression, and the relevance of collective access to information, it is not a conflict between purely private interests, but faces demands that make the general interest of the community – access to information, prohibition of prior censorship, freedom of expression – and the imperatives that protect the fundamental rights of the individual, which also make up the public interest.

In this regard, the Office of the Rapporteur for Freedom of Expression of the Organization of American States has said that "freedom of expression applies to the Internet in the same way as to all media," adding that "states have the obligation to promote universal access to the Internet to guarantee the effective enjoyment of the right to freedom of expression. Access to the Internet is also necessary to ensure respect for other rights, such as the right to education health and work, the right of assembly and association, and the right to free elections"[366].

In short, prior legal definition, subject to criteria of reasonableness and pluralism, illegal content could only be prosecuted with all the

366 Joint Declaration on Freedom of Expression and Internet, June 1, 2011, points 1.a and 6.a, respectively. See <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849>. Cf. CSJN Argentina, in R., MB vs. Google and other.

legal guarantees that generally establish democratic constitutions. In our opinion, it must be the judges who must order the kidnapping, closure or detention of publications, content or persons who have allegedly incurred in a crime of dissemination of illegal content[367].

18.11 References

Alexy, R. (2005). Los Derechos Fundamentales en el Estado Constitucional Democrático, en Carbonell, Miguel (Edit.), Neoconstitucionalismo(s), 2ª Edición, Trotta, Madrid.

Alexy, R. "Theorie der Grundrechte", 1994 (segunda edición), pág. 327 traducida por Garzón Valdés, Ernesto como "Teoría de los derechos fundamentales" (Centro de Estudios Constitucionales, Madrid, 2002 (3ª, reimpresión), p. 349 y ss.

Belli, L., Schwartz, M. & Louzada, L. (2017). Selling your soul while negotiating the conditions: from notice and consent to data control by design. In Health & Technology Journal Springer – Nature. Topical Collection on Privacy and Security of Medical Information. Vol 7, nº4. 453-467 <https://link.springer.com/article/10.1007/s12553-017-0185-3>.

Carrascosa López, V. (1992). Derecho a la Intimidad e Informática, en Informática y Derecho UNED, pag. 23.

Cooley, M. (1895). The elements of Torts, Editorial Callaghan.

Correa, C. y otros. (1987). Informática, Libertad y Derechos Humanos, en Correa, Nazar Espeche, Czar de Zalduendo y Batto, "Derecho Informático", Depalma, Buenos Aires.

Corte Interamericana de Direitos Humanos (CIDH). (1985). "La colegiación Obligatoria de Periodistas (A instancia del Gobierno de Costa Rica)", Opinión Consultiva 5/85, numeral 29.

Corte Interamericana de Direitos Humanos (CIDH). La colegiación obligatoria de periodistas (arts. 13 y 29, Convención Americana sobre Derechos Humanos), opinión consultiva OC-5/85 del 13/11/1985, Serie A, nro. 5, párr. 30).

Corte Suprema de Justicia de la Nación, 15/10/1998, "Urteaga, Facundo R. c/ Estado Mayor Conjunto de las Fuerzas Armadas", voto del Dr. Santiago E. Petracchi, LA LEY, 1998-F, 237.

CS E.E.U.U., 26/06/1997, "Janet Reno, Fiscal General de los Estados Unidos de America, et al, apelantes c/ American Civil Liberties Union, et al No. 96-511, elDial AA1748 (texto completo en español) (1997 U.S LEXIS 4037).

CS, 12/03/1987, "Costa, Héctor R.", Fallos 310:508.

CS, 19/11/1991, "Vago, Jorge A.", Fallos 314:1517.

367 This seems the criterion of the bill, approved by the Argentine Senate and considered by the Chamber of Deputies, at the time of writing these lines, as well as what emerges from the Framework Civil Law of Brazil and the latest Law of Property Intellectual of Chile.

Derecho Público Contemporáneo Nº 7, revista de la Agrupación de Abogados de la Contraloría General de la República de Colombia.

Fernández Sessarego, C. (1992). El Derecho a la Identidad Personal y otras figuras, Ed. Astrea, Bs. As., p.153.

Hassemer, W. y Sánchez, A.C. (1997). El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales, Editores del Puerto, Buenos Aires, p. 172.

Katz vs. United States. (1967). 389 US 347,351. <http://supreme.justia.com/us/389/347/case.html>.

Kommers, D. (1989) The Constitutional Jurisprudence of the Federal Republic of Germany, Durham, Londres, pág. 332 y voto Dr. Petracchi en "Urteaga".

Martino, A. (2000). E-Comerce y Derecho hoy. La experiencia de la Comunidad europea, Ecomder. <http://ecomder.com.ar>.

Molina Quiroga, E. (2015). Responsabilidad de los buscadores. Análisis del tema a la luz del derecho comparado y la jurisprudencia de la Corte Suprema de Justicia, La Ley Online; Revista Código Civil y Comercial (Edición Especial) La Ley, octubre 2015, III, 173/182. Cita Online: AR/DOC/2974/2015;

Molina Quiroga, E. (2017a). El derecho a la imagen y la responsabilidad de los buscadores. Una nueva sentencia de la Corte, LA LEY 03/10/2017, 4, AR/DOC/2535/2017, entre otros.

Molina Quiroga, E. (2017b). Redes sociales, derechos personalísimos y la libertad de expresión, LA LEY 16/08/2017, 5, AR/DOC/2149/2017.

Relatoría para la Libertad de Expresión de la Organización de los Estados Americanos. (2011). Declaración Conjunta sobre Libertad de Expresión e Internet, 1° de junio de 2011.

Stiglitz, R.M. (1987)., LA LEY, 1987-E-859.

Warren, S.D. & Brandeis L.D. (1890). The Right to Privacy. Harvard Law Review, Vol. 4, No. 5, pp. 193-220. <http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>.

19 Big Data is Us: New Technologies and Personal Data Management

Eduardo Magrani and *Renan Medeiros de Oliveira*

Abstract

This article seeks to present a critical view on the use of personal data in the current hyper connectivity scenario, bringing to the surface, as an alternative, the possibility of self-management of data, based on a specific project. We will present, first of all, a panorama of privacy in the 21st century, highlighting that it is a multifaceted right that has gained new contours in the face of contemporary technologies and that has challenges still unanswered. Second, we will deal with the notion of *Big Data*, a term that describes any voluminous amount of structured, semi-structured or unstructured data that has the potential to be exploited to obtain information. We will try to highlight, also, the idea that *Big Data* is us and we have incentives to take back control of that information. In a third moment, we will make an exposition about the personal data management project called *My Data*. We will finish this analysis with the defense that a project of this bias can be an effective alternative to protect the right to privacy in the contemporary world.

19.1 Introduction

Technology has advanced rapidly and has helped to improve the way we live. In addition to interfering with the way individuals act, it changes the way people relate to each other, to business, and to government. The many changes highlight the need to give importance to the individual and to have a multisectoral dynamic to build a sustainable Internet governance.

It is undeniable that new technologies bring benefits. As a consequence, however, regulatory and ethical questions arise linked to its use.

With more and more connected devices, related to the scenario that is being called the Internet of Things ("*or IoT*[368]), various risks and challenges arise, such as those related to the right to privacy.

The data generated through the use of these innumerable intelligent devices are collected and stored by the companies, which do not always act transparently. The terms of use and service are usually extremely technical and unintelligible for the general population. It is not uncommon for the purpose of the data to be hidden from the users themselves, who have no control over the information that refers to them.

Given the voluminous amount of data produced daily, this becomes even more worrisome, especially since the phenomenon of "*Big Data*[369]" goes far beyond an entanglement of data, being essentially relational. It is necessary to keep in mind that the Big Data is us and, therefore, we must have a critical conscience about it and think about possibilities of regaining control over our personal data.

With the possession and availability of our data, companies use techniques such as tracking, profiling and targeting to direct their marketing policies of the way we live and our needs, or what they make us believe is a necessity.

In this way, discussions regarding the right to privacy are intrinsically connected to discussions about the use and management of data. Technological progress requires adaptations of the legal system to new scenarios, which can occur, for example, through legislative action or interpretive activity. These solutions are not always effective: on the one hand, the sociopolitical conjuncture and the technological pattern change much more rapidly than the legislation is able to accompany and, on the other hand, the judicial interpretation of the rulers can acquire paternalistic and corporate character if it is distanced from the will of the individuals.

---

368 In general, the Internet of Things can be understood as an ecosystem of physical objects interconnected through the Internet, using small and embedded sensors, creating an omnipresent (ubiquitous) computing ecosystem, aimed at facilitating people's daily life, introducing functional solutions in day-to-day processes.

369 *Big Data* it is an evolving term that describes any voluminous amount of structured, semi-structured or unstructured data that has the potential to be exploited to obtain inferences and generate profits.

Thus, new ways of protecting the right to privacy and increasing the control that Internet users have over their own data have emerged as an alternative.

The MyData project was created with this in mind. Basically, it is a system whose objective is to place the individual at the center of personal data so that they themselves have control over the information produced about themselves, dissociating themselves from the abusive control of data currently exercised by the companies. That is to say, a perspective centered on the human being is adopted, and not more on the things or on the information itself. In the current management model, the data belongs to those who collect it. The individuals themselves to whom the information refers do not even know, in general, the purpose for which they are used, which creates serious problems for privacy and goes against the principle of transparency. The new system seeks to create a scenario in which users have their human rights respected in the digital environment and can have control over their data, while creating no barriers to innovation for companies that can develop innovative services based on mutual trust

The present study is intended to analyze this project more closely and seeks to rate the benefits that can lead to the protection of privacy and the taking over control of personal data by the individuals themselves. To do this, we will first make a brief overview of the right to privacy, its contours and the impacts that new technologies generate on it. In a second approach, the aspects related to Big Data will be subject to analysis, so that a more detailed notion about the production and storage of data is made. Thirdly, we will present in more detail the personal data management project mentioned above. We conclude with an analysis of how this project tends to contribute to the protection of privacy in the present against new technologies.

19.2 The challenge of privacy in the hyper connected world

The protection of privacy is a fundamental part of societies that claim to be democratic, and is intended as a fundamental right in the

Inter-American Convention on Human Rights[370] and in the Universal Declaration of Human Rights[371] International treaties on the subject, in general, deal with privacy under the aspect of non-interference in private family life, correspondence and communications, as does the Brazilian Federal Constitution of 1988. The interpretation of privacy, however, has been changing substantially in recent years and that right has gained new contours[372].

The right to privacy consists of a complex value (Post, 2001) that has different meanings and different aspects that characterize it. Among these aspects, we have the traditional vision of Samuel D. Warren and Louis D. Brandeis (1890) of the right to be left alone, which implies the control of the individual over information referring to his personal life (Sarlet, Marinoni & Mitidiero, 2012). As Sarlet points out on the basis of Vital Moreira and Canotilho, the right to privacy implies the right to prevent strangers from gaining access to information about private life and not to disclose it (Ibid.). Another aspect of the right to privacy is from the standpoint of protection against interference from others, which implies the right that the individual has to be left alone in order to live his life with a minimum degree of interference, from the standpoint of the secret or secret of certain information and, finally, from the perspective of control over information and personal data[373].

With social and technological development, different facets of privacy have emerged[374] and new conflicts and problems[375] have appeared – such as the debate about the right not to take knowledge about

370 In the document, privacy is linked to the protection of honor and dignity. Article 11: "1. Article 1. 2. No one may be subject to arbitrary or abusive interference in his private life, in that of his family, in his home or in his home in his correspondence, nor of illegal offenses to his honor or reputation. 3. Everyone has the right to the protection of the law against such interference or such offenses."

371 Artigo 12° "Nobody will suffer arbitrary interference in his private life, in his family, in his home or in his correspondence, nor attacks on his honor and reputation. Against such intrusions or attacks every person has the right to the protection of the law."

372 As Rodotà (2008: 23) states, "[t] he new dimensions of the collection and treatment of information caused the multiplication of calls to privacy and at the same time increased the awareness of the impossibility of confining the new issues that arise within the institutional framework traditionally identified by this concept".

373 On the different concepts of privacy, v. Leonardi (2011).

374 Mulholland (2012: 3), for example, presents three conceptions about the right to privacy, which are, "(i) the right to be left alone, (ii) the right to have control over the circulation of personal data, and (iii) the right to freedom to choose people of existential character "and adds to this list the right not to have knowledge of a certain personnel".

375 Review, on the subject, Sloan & Warner (2014) and Madden (2012).

personal data[376], the discussion about unauthorized biographies[377] and the right to non-tracking[378]. In the information society, privacy must be understood in a functional way, in order to ensure a subject, the possibility of "knowing, controlling, straightening, interrupting the flow of information related to it" (Rodotà, 2008, p 92). In this sense, Stefano Rodotà (2008: 92) defines privacy "as the right to maintain control over one's own information".

The right to privacy has no ambiguous concepts. The notion of private life has been expanded due, among other factors, to the development of technology. Therefore, the concept goes on to encompass the "set of actions, behaviors, opinions, preferences, personal information, on which the interested party intends to maintain exclusive control" (Rodotá, 2008, p.92). The conception of what is private, tends to encompass the set of activities and situations of a person who has a communication potential, verbal and non-verbal, and which can, therefore, be translated into information "(Doneda, 2006: 153).

The technological factor has a prominent role, since with the improvement of storage capacity and communication of information, new ways of organizing, using and appropriate the information (Doneda, 2006, p. 153).

As Danilo Doneda (2008, pp. 153-154) points out, "this growing importance is reflected in the fact that a considerable part of individual freedoms today is materialized through structures in which communication and information play a role relevant.

The technological development allows the creation of profiles of behavior that can even be confused with the person[379]. Such

376 Mulholland presents a case in which a patient had taken to investigate, among others, the existence of the Hepatitis C virus and received, because the blood test conducted by the laboratory was other than not requested, the positive result of the anti-HIV test. For Mulholland, "disclosure to the unsolicited data person constitutes a violation of their right not to know and undoubtedly generates the right to compensation for moral damages." (Mulholland, 2012: 11).

377 Cf. Moraes (2013).

378 Cf. Magrani (2017).

379 As Danilo Doneda (2006: 173) points out, in the profiling technique, "personal data are treated, with the help of statistical methods, artificial intelligence techniques and others, in order to obtain a" metainformation, which would consist of a synthesis of habits, personal preferences and other records of this person's life. The result can be used to draw a picture of the future trends, behaviors and destinies of a person or group."

profiles, together with the manipulation of harvested data, can generate serious impacts on freedom:

> "Another technique still refers to a method of collecting personal data, known as data mining. It is the search for correlations, recurrences, forms, trends and significant patterns from very large amounts of data, with the help of statistical and mathematical tools. Thus, from a large amount of information in raw and unclassified state, information of potential interest can be identified". (Doneda, 2006: 176)

Thus, if, on the one hand, technology brings undeniable benefits to society as a whole, it creates, on the other hand, problems to the protection of privacy. Although technology helps to shape a richer private sphere, it contributes to making this sphere more and more fragile and exposed to threats, from which derives the need for the continuous strengthening of its protection (Rodotà, 2008: 95).

The need for greater protection of personal data is deepened in the Internet of Things scenario[380].

In this context, the increasing connectivity with the most diverse technology devices generates a practically inexhaustible source of information about the daily life of the users of said devices. In view of the fact that when speaking of privacy we have personal information in mind (Ibid., P. 93), it is essential to devote special protection to the data and information generated through Internet connections and devices connected to the Internet[381].

---

380 "With the advent of new technologies, especially the development of biotechnology and the Internet, access to sensitive data and, consequently, its dissemination, have been extremely facilitated. As a result, there is an expansion of potential forms of violation of the private sphere, to the extent that it shows the ease by which unauthorized access by third parties to such data is possible. With this, the protection of privacy is seen not only as the right not to be disturbed, but also as the right to have control over personal data and, thereby, prevent its unwanted circulation." (Mulholland, 2012: 3).

381 In a similar sense, Doneda (2008, p.362) affirms that personal data "deserve particular attention, be it for the dynamics of its content or for the new scenario it seeks to regulate, marked by the strong presence of technology". Carlos Affonso de Souza (2000, p.23) also positions himself in that sense, stating that "the threats to the right to privacy were severely increased as technological progress allowed greater facilities for the individual. The processing of information by computers allows not only its rapid processing for suitable purposes, but also for the rapid crossing of confidential data or the interception of them in a network, for example. The Internet, an example of such progress, is, therefore, the scenario where the new guardianship demanded by the need for personal privacy is currently being discussed."

Brazil, unlike the countries of Latin America[382] and Europe[383], does not yet have a sufficient legislative framework to guarantee the protection of privacy[384]. There are bills currently being processed in the National Congress seeking to approve a general law protecting privacy and personal data[385].

However, protection should not be given only through legislation, since laws are limited in time due to rapid social changes. Thus, and taking into account that privacy should also be understood as positive freedom, it is fundamental to create mechanisms that give individuals the power to control their own data, the processes to which they will be subjected, and the purposes underlying their use. One of the possible alternatives to protect privacy and empower individuals to control their data is the personal management of data, a concept that will be presented in detail below.

19.3 We are *Big Data*: between economic exploitation and personal control of data

Every day, we connect to the Internet through devices that have the capacity to share, process, and store and analyze a huge volume of data. This situation generates what we know as *Big Data*,

382 There are laws enacted, for example, in Argentina, Chile and Colombia (Banisar, 2016).

383 In Europe, all countries, except Belarus, have personal data protection laws (Banisar, 2016). On this continent, with the leaks on US surveillance programs, MEPs acted to strengthen the existing rules since 1995. Thus, they voted for the reform of European standards on the protection of personal data, seeking to ensure Internet users greater control over their data and subject transfers of personal data processed in the European Union outside it to more severe requirements (Redação, 2014).

384 The Brazilian Constitution provides for recognition of the right to privacy, privacy (Article 5, paragraph X) and the inviolability of data (Article 5, paragraph XII), and notes the habeas date as a suitable instrument to ensure the protection of information and, personal data (article 5, subsection LXXII). There is also legislative protection at the infra-constitutional level. The Civil Code of 2002 protects private life (Article 21) and the Consumer Protection Code devotes Section VI to the protection of data banks and consumers' cadastres. Finally, the Internet Civil Framework, in force since 2014, develops the protection of privacy and data as principles to be observed in the Internet discipline as a pillar of the Law (Article 3, items II and III). Articles 7 and 10 of the Civil Framework also address the issue. This regulation, however, is insufficient to protect personal data and privacy in its most diverse facets.).

385 Between the years 2013 and 2014 the PLs n ° 330/2013, No. 181/2014 and No. 131/2014 were proposed, which had on the protection of personal data in general and the supply of data of citizens and / or Brazilian companies to organizations foreigners, fruits of the CPI of the Espionage carried out by the Federal Senate. In 2015, these three projects were appeased and processed together until today.They also deal together with PL No. 4060/2012 and Proposed Draft No. 5276/2016. Project No. 5276/2016 brings important principles for the protection of privacy and personal data to be effective, such as the principle of purpose, the principle of adequacy and the principle of necessity. The PL suffered a strong influence from European regulation, keeping innumerable similarities with the *General Data Protection Regulation*, of 2016.

which is an evolving term that describes any voluminous amount of structured, semi-structured or unstructured data that has the potential to be exploited for information (Lane, 2014).

The first property in relation to *Big Data* consists of the growing volume of data (Rijmenam, 2015). A recent investigation by Cisco (2016) estimates that, in the next few years, *gigabytes*[386] will be exceeded and the calculation of the amount of data will be done in the order of *zettabyte*[387] and even in *yottabyte*[388].

Another property involves high speed (Ibid.) with which the data is produced, analyzed and visualized. In addition, the variety of data formats represents an additional challenge. This feature is enhanced by the different devices responsible for collecting and producing data in various areas. The information produced by a mechanism that monitors the temperature is very different from those obtained in social networks, for example. In addition, most of the data found are not structured (Ibid.; Molaro, 2013).

The concept of *Big Data*[389] can imply, together with the concept of Data Science, the ability to transform raw data into graphs and tables that allow the understanding of the phenomenon to be demonstrated. It is important to mention that, in a context in which decisions are made more and more on the basis of data, it is extremely important to guarantee the veracity of this information (McNulty, 2014).

In the words of Maike Wile dos Santos (2017), "*Big Data* is more than an entanglement of data, because it is essentially relational." Although it is not a new phenomenon, "what the Internet did was give it a new dimension, transforming it. To understand these transformations well", says Wile, "we need to understand that Big Data is us."

---

386 *Gigabyte* is a unit of measurement of information that equals 1 trillion *bytes*.

387 *Zettabyte* is a unit of measurement of information that is equivalent to 1 sextillion *bytes* (1021).

388 *Yottabyte* is a unit of measurement of information that is equivalent to 1024 *bytes*.

389 For José Carlos Cavalcanti, the concept of Big Data applies to information that cannot be processed or analyzed using traditional processes or tools. Cavalcanti mentions as basic characteristics of the concept of *Big Data*: volume, variety and speed (the so-called 3 Vs, previously created concept), also recognizing the "veracity" as another possible characteristic defended by other authors (Cavalcanti, 2016). The 3 Vs are used by the doctrine to refer to *Big Data* since mid-2010. Cf. Global Pulse, 2012, p. 13 e ss.

The combination between intelligent objects and *Big Data* can significantly alter the way we live (FTC Staff Report, 2015). Some research (Barker, 2014) estimated that, by 2020, the number of interconnected objects will exceed 25 billion, and may reach 50 billion smart devices. The projections for the impact of this scenario of hyper connection in the economy are impressive, corresponding, globally, to more than US $ 11 trillion in 2025 (Rose, Eldridge & Chapin, 2015).

Intelligent and interconnected objects can help us in solving real problems. From the point of view of the consumers, the products that today are integrated with IoT technology are of the most varied areas and have diverse functions, from household appliances[390], means of transportation to toys.

Today there are also garments that have IoT connectivity, forming part of a category called *wearables*. These technologies consist of devices that connect to each other producing information about the users and the people around them. Among the main products stand out the bracelets and shoes that monitor the user's physical activity, as well as smart watches and glasses that aim to provide the user with an immersive experience in their own reality (Landim, 2014; Darmour, [sd]; O'Brien, 2016).

However, transforming an analog object into an intelligent one, besides making the product more expensive and subjecting it to failures that it would not have a priori, can also generate risks in relation to security and privacy[391]. We are talking about a context that involves a massive volume of data being processed in the scale of billions of data daily, allowing it to be possible to know more and more individuals in their habits, preferences, desires and trying, thus, to direct their choices.

This need has been well seen by the market, which has explored the possibility of personalization and automatic customization

390 "Smart refrigerators are perhaps the most common example when we talk about the Internet of things. The Samsung RF28HMELBSR / AA refrigerator, for example, is equipped with an LCD screen capable of playing the screen of your smartphone in the refrigerator. It is possible to play videos and songs, check the weather forecast and even make purchases online while checking in the fridge the items that need to be purchased. The refrigerator brings an application called Epicurious, which allows the consultation of recipes online "(Nascimento, 2015).

391 On the subject, see Roman (2010).

of content on digital platforms, including capitalizing on that filtering with targeted advertising through the tracking of cookies and retargeting or programmatic media (*behavioral retargeting*) (Oliveira, 2016).

Today, there is no clarity in the treatment given to the data (Accenture, [sd]). The aspects of collecting, sharing and the potential use of them by third parties are still unknown to consumers. This has the potential to impact and, in a certain sense, already impacts (Bolton, 2016; Consumer Technology Association, 2016; Accenture, [sd]; Plouffe, 2016) the confidence of the users in the connected products (Meola, 2016).

It also highlights the fact that security flaws open space for attacks by looking at the access to information generated by the devices themselves. In addition, smart devices, when they are invaded, can cause problems not only for the device itself, but also interfere with the network's own infrastructure. It was what happened at the end of 2016 with the DDoS attack (Cobb, 2016), an occasion in which hackers managed to suspend several sites invading the servers through security cameras, revealing the vulnerability of those devices. Therefore, issues related to the security and protection of personal data are equally important for the IoT to consolidate as the next step on the Internet.

Given this scenario, one of the most important issues related to the protection of personal data concerns who controls them and who has access to them. In the current model, technology companies are endowed with this control and have such access. The individual himself, in relation to whom the information is collected, often does not even know that his data is being stored and, when he knows, it is not unusual for him to be unaware of the purpose of such collection and storage. A society that is transparent and democratic cannot do without clear and fair data management. It is necessary to give individuals control over their own data and empower them to decide what, with whom, when and for what to share.

19.4 Personal data management projects

Online interaction is a constant presence in the lives of almost all individuals. In the hyper connected contemporary world, information and news are increasingly being obtained through the Internet. The hiring of products and services is increasingly done through digital means, as well as the establishment of social and professional contact. This, however, many times, goes unnoticed by users, who do not realize the digital trail they produce on themselves. The data produced, not rarely, are stored for a long period of time. The control of this trail has become a technological and social problem, since from its analysis it is possible to obtain information about the behavior, preferences and personal needs of a certain person and even foresee their future actions (Sjöberg, 2016).

An example linked to the forecast of future actions of people based on their purchasing habits that demonstrates the danger of the free use of personal information is the crossing of data made by sales companies. Target creates an identity for each consumer through the information obtained when the customer uses the credit card, a promotional coupon, contacts the SAC or visits the online store. The company realized that if a woman buys some items together or in larger quantities, such as odorless lotions, coconut butter lotions, zinc and magnesium supplements and a large bag, there is an 87% chance that she is 3-months pregnant (Rodrigues, Santos, [sd]; Redação, 2012). An interesting case occurred in 2012, when the company delivered discount coupons by mail to a woman, but her father received them, which ended up anticipating the disclosure of the news to the father (Duhigg, 2012).

As if data collection about individuals and the formation of individual profiles wasn't enough, individuals usually do not have access to the personal data generated about themselves. Large Internet companies, such as Google and Facebook, centralize the information collected and encourage people to use only their tools, since there is no exchange of information between them, which goes against market competition and innovation. The user does not control their personal data (Sjöberg, 2016). As highlighted by Belli, Schwartz and Louzada (2017), one of the recently proposed

technical solutions for this problem points to personal data centered on the human being, that is, the individuals themselves should control their data.

Personal data have an increasingly significant social, economic and practical value, but their application and wider use is often confused with negative forecasts of a future devoid of individual privacy (Poikola, Kuikkaniemi, & Honko, [sd]). MyData consists of a structure with a system centered on the human being (different from the current system centered in the organization) and rights-based data management.

Individuals must be at the center of the control of their own data and their digital human rights must be strengthened at the same time that companies have the possibility of developing innovative services based on mutual trust (Ibid., P.1). MyData allows the collection and use of personal data to maximize the benefits obtained, minimizing lost privacy. Thus, these valuable data will allow individuals to interact with suppliers, who can offer data services and improve consumption (Ibid., Pp. 3-4).

This interoperable infrastructure approach based on MyData provides individuals with data-driven services and greater privacy and transparency, increases freedom of choice and empowerment, among other benefits. Consent management is the main mechanism to allow and apply the legal use of the data. In this model, consent is dynamic, easy to understand, machine readable, standardized and managed in a coordinated manner. A common format will allow each individual to delegate data processing to third parties or reuse the use of data in new ways (Ibid., P.7).

MyData equips individuals to control who uses their personal data, stipulate for what purposes they can be used and give informed consent in accordance with personal data protection regulations. Data flows become more transparent, broad and manageable. Users can also turn off information flows and withdraw consent. Finally, machine-readable consent can be displayed, compared and processed automatically (Ibid., P.8).

In addition, MyData can be considered useful for companies, because it will help to integrate complementary services of third

parties in its main services; Simplify operations within current and future regulatory frameworks and allow the use of data for exploratory purposes; enabling the creation of new businesses based on data processing and management (Ibid., p.8).

It is interesting to note that MyData is complementary to Big Data, and vice versa, because, without addressing the human perspective, many of the potential innovative uses of Big Data are incompatible with the regulations currently in force. This approach has three principles that require maturation:

> **(i) control over data centered on the human being:** The human being is an actor in the management of their lives online and offline and has the right to access their personal data and control their "privacy settings" (Belli, Schwartz & Louzada, 2017, p.8)[392], as much as necessary to make them effective;
>
> **(ii) usable data:** it is necessary that the personal data are technically easy to access and readable by the APIs (*Application Programming Interfaces*). MyData converts data into a reusable resource to create services that help individuals manage their lives;
>
> **(iii) open business environment:** The infrastructure allows the decentralized management of personal data, improves interoperability, facilitates the compliance of companies with data protection regulations and allows individuals to exchange service providers without data blocking. Thus, "by meeting a common set of personal data patterns, companies and services allow people to exercise freedom of choice between interoperable services," preventing people from having their data blocked in "services belonging to a single company because they cannot export them "and take them to another supplier (Belli, Schwartz & Louzada, 2017: 460)[393].

392 Free translation.

393 Free translation.

MyData is a more robust infrastructure compared to simple APIs. The data aggregator that is being used today is evolving naturally outside the API economy, but it has major disadvantages: the lack of interoperability between data aggregators and the fact that the current source of aggregators does not necessarily recognize privacy or engages in a transparent relationship with individuals. The adoption of the MyData approach can lead to a systemic simplification of the personal data ecosystem. This simplification can be done gradually, since the platform can be developed and implemented in stages, together with the evolution of the API economy and the existing data aggregator model (Poikola, Kuikkaniemi, & Honko, [sd], p.6).

Finally, it is interesting to observe how the MyData architecture works: based on interoperable and protocolized accounts:

> "The model provides individuals with an easy way to manage their personal data from a single location, although the data is created, stored and processed by hundreds of different services. For developers, the model facilitates access to data and eliminates dependency on specific data aggregators. The accounts will generally be provided by organizations that act as MyData operators. For organizations or individuals willing to be independent of the operator, it will also be technically possible to host individual accounts, similarly to how some people currently choose to host their own email servers. "(Ibid. P.6)

Interoperability is the main advantage provided by MyData, but it is also the main challenge, because it requires more standardization, more trust networks and data formats. In the MyData architecture, data flows from a data source to a service or application. The main function of a MyData account is to enable consent management. APIs allow interaction between data sources and users (Ibid. P.8). As already mentioned, the standardized architecture makes accounts interoperable and allows individuals to easily exchange operators.

19.5 Final considerations: personal data management as an alternative to protect privacy

The current model by which personal data are managed goes against the right to privacy and transparency, in addition to reducing the power of choice of individuals.

As Belli, Schwartz and Louzada (2017, p. 455-457) note, the terms of use of the online services offered by companies are long texts that are about to discouraging readability by the user and have technical terms that cannot be understood by the population without specific technological knowledge. The same applies to privacy policies.

Belli, Schwartz and Louzada (2017: 458) highlight that research done in 2017 by professors from the Universities of Michigan and Connecticut (Obar, Oeldorf-Hirsch, 2016) involved 543 participants and showed that 74% of the users did not they read the privacy policies and those who do spend, on average, only 74 seconds in that task. The average reading time of the terms of service is 51 seconds. For McDonald and Cranor (2008), the reading time of the privacy policies is a form of payment. The reading of all the policies would take 201 hours per year and would be equivalent to $ 3,534 per year and for each American user. Under the national perspective, the careful reading of these policies would mean that the time spent equaled some 781 billion dollars a year.

People do not know the value of their data and, most of the time, do not want to deal with the complication of managing it (Data is Giving, 2017). With this, companies use the data however fits their interests, which may involve the sale and transfer of information to third parties, increasing the risk of leakage and, therefore, privacy violation. The fact that the data are non-rival, that is, can be used at the same time by more than one person or algorithm, creates complications, such as giving them a destination different from that to which the user expressed consent. In this scenario, the data belongs to those who collect it, and not to the person to whom they refer. Researchers from the Technology and Society Center of the Getúlio Vargas Foundation conducted a study comparing 50 terms of use and service of online platforms analyzing how

they handle the rights to freedom of expression, privacy and due process of law. The authors concluded that, in this light, the terms are deficient.

The main objective of companies when adopting them is "to minimize exposure to liability, rather than detailing their obligation to guarantee respect for certain rights" (Venturini *et al*., 2016, p.77), which explains both the vague and "ambiguous" terminology adopted as "the tendency to provide users with as little information as possible, particularly in the crucial aspects for the protection of human rights" (Ibid., p 74). In this sense, the study showed that only 12% of the platforms foresee in their terms of use the possibility that after the cancellation of the account, personal data generated by users or collected in another way may be excluded. 60% of the platforms do not even provide information on the subject, while 10% expressly state that they do not allow the total exclusion of the data. 18% provide contradictory information in this regard (Ibid.). Another interesting example is the fact that 62% of companies have clauses that require the consent of users for the exchange of data for commercial purposes (Ibid.), which leads us to question whether the consent given by the user is effectively informed.

The problems related to privacy and data management by companies lead us to understand that the currently existing consent model has failed. For that model, personal data became a currency that can be used by individuals to access content online. In other words, in order to enjoy services, individuals agree that their personal data are accessed, processed and disclosed (Belli, Schwartz & Louzada, 2017: 456). Notice what Luca Belli, Molly Schwartz and Luiza Louzada explain:

> "One could argue that the N & C [notice and consent] scheme is based on a series of dubious claims. First, it assumes that the individuals who express their consent for PP [Privacy Policies] and ToS [Terms of Service] behave as rational economic subjects, with time and knowledge to carefully analyze the content of each contract. Second, it postulates that individuals possess the bargaining power necessary

> to freely accept the provisions included in contractual agreements defined unilaterally by the providers. Such assumptions clearly overestimate both the bargaining power and the degree, quality and intelligibility of the information available to people who are weighing the costs and benefits of providing their consent "(Ibid, p.456)[394].

The ineffectiveness of the terms of service and the absence of informed consent are even clearer in the Internet of Things scenario. The 2017 Unisys Security survey involved citizens from 13 countries and showed that Brazilian are the most willing to provide their personal data in exchange for the comfort of connectivity between their devices (Soprana, 2017). As an example, 88% of Brazilians are favorable to the placement of sensors in the luggage to have communication with the airport system so that their items are more easily located; 83% accept that health information obtained through pacemakers, among other devices, be shared with doctors; and 50% agree with supplying health insurance companies with information related to the physical activities obtained from watches.

The great interest of companies for personal data is mainly due to their economic usefulness, so that, in this century, they are equivalent to what oil meant in the last century. In addition, data is transported to thousands of computers that extract certain values, such as patterns, predictions and other *insights* on the digital information of individuals, which can be used in marketing policies, artificial intelligence mechanisms and "cognitive" services (Data is Giving, 2017).

Digital information comes from different sources and is extracted, refined, valued, bought and sold in different ways. This changes the rules of the market and demands a new regulatory approach (Data is Giving, 2017). It is necessary that individuals have control over their data and are aware of the destination that will be conferred after the authorization of use, which, among other benefits, will increase the freedom of choice of users and empower them.

394 Free translation.

In addition, it is necessary to face the challenge of making people understand the value of their data and that they are compensated for the granting of information (Ibid.).

User confidence in the regulation of privacy and freedom of information is intimately connected to democracy, as Denham (2017) points out, and the digital economy is dependent on that trust. Privacy and innovation do not have to be divergent. The task of developing an infrastructure in which these two elements are convergent is difficult and requires high levels of dedication. However, the task, which is not impossible, is essential: privacy demands the highest level of innovation. It is necessary that privacy and innovation go together, so that they do not collide and that one does not hinder the evolution of the other. They can and should walk parallel, and that is what the public expects and the law demands (Denham, 2017).

Taking into account these needs for change, the previously described project has been developed to give the individual power over their information and make them the owners of their data, instead of the companies that collect them. Projects of this kind can be the solution to overcoming an Internet dominated by oligopolies, techniques of *profiling* and generalized surveillance (Abiteboul, André, & Kaplna, 2015).

The MyData project starts from the current context of data management, which is harmful to privacy and transparency, and seeks to empower individuals, giving them back control over their own data. We are in constant digital interaction and leave traces with every click we make. Most of these interactions are stored for a long time, which creates a digital history of people and analyzes their behaviors, preferences, needs, even anticipating future actions. In general, this data is not available to the users themselves and they do not even know what information is being collected and stored. Individuals do not control their own data, companies do. Therefore, the project aims at giving people control over their data and allowing them to decide, based on clear information and the useful organization of their data, if they want to hire a certain product or service.

The system that is being developed has its central vision focused on the human being, but it is also useful for companies, which will be able to create more profitable products and services for individuals. A point that also deserves to be highlighted is the fact that the project is not limited to proposing a data gathering in a single place, but it presents a model through which individuals can understand and organize their data to obtain a clearer visualization and understanding of the information contained in the systems. However, adherence to this approach remains embryonic. Large companies linked to technology and data management, such as Facebook and Google, have no interest in the advancement of projects like this, since it is extremely disruptive to their business models. Therefore, besides promoting this type of projects, we must think of ways to make users know the value and importance of their data and know that they can have control over them, defining who will use them, when and what for.

The Internet has given a new dimension to personal information and privacy and generated what we know as Big Data, which goes far beyond an entanglement of data: Big Data is us. It is from the recognition of the importance of our data and the development of secure projects that give the individual control over their information that we can ensure effective protection of privacy in the face of new technologies.

19.6 References

Abiteboul, S., André, B., & Kaplan, D. (2015, May). Managing your digital life. *Communications of the ACM*, *58*(5), 32-35.

Accenture. ([s.d.]) *Digital trust in the IoT era*, [s.d.]. Retrieved from <https://www.accenture.com/t20160318T035041__w__/us-en/_acnmedia/Accenture/Conversion-Assets/LandingPage/Documents/3/Accenture-3-LT-3-Digital-Trust-IoT-Era.pdf>.

Banisar, D. (2016). National Comprehensive Data Protection/Privacy Laws and Bills 2016. *ARTICLE 19: Global Campaign for Free Expression*. Retrieved from <https://ssrn.com/abstract=1951416>.

Barker, C. (2014, November 11). 25 billion connected devices by 2020 to build the Internet of Things. *ZDNet*. Retrieved from <https://www.zdnet.com/article/25-billion-connected-devices-by-2020-to-build-the-internet-of-things/>.

Belli, L., Schwartz, M., & Louzada, L. (2017). Selling your soul while negotiating the conditions: from notice and consent to data control by design. *Health Technology*. Retrieved from <https://link.springer.com/article/10.1007/s12553-017-0185-3>.

Bioni, B. (2014). A produção normativa a respeito da privacidade na economia da informação e do livre fluxo informacional transfronteiriço. In A. Rover, J. Cella, & Ayuda, F. *Direito e novas tecnologias* (pp. 59-82). Florianópolis, Brasil: CONPEDI.

Bobbio, N. (1997). *Igualdade e liberdade*. Tradução: Carlos Nelson Coutinho. 2. ed. Rio de Janeiro, Brasil: Ediouro.

Bolton, D. (2016, September). 100% of reported vulnerabilities in the Internet of Things are Avoidable. *Applause*. Retrieved from <https://arc.applause.com/2016/09/12/internet-of-things-security-privacy/>.

Cavalcanti, J. (2016). The new ABC of ICTs (analytics + Big Data + cloud computing): a complex trade off between IT and CT costs. In: J. Martins, & A. Molnar (Org.). *Handbook of research on innovation in information retrieval, analysis and management*. Hershey, United States: IGI Global.

Cavoukian, A. (2012). Privacy by Design. *IEEE Technology and Society Magazine*. Retrieved from

Cisco. (2016, June). The zettabyte era: trends and analysis. *Cisco*. Retrieved from <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html>.

Cobb, S. (2016, October 24). 10 things to know about the october 21 DDoS attacks. *We Live Security*. Retrieved from <https://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/>.

Consumer Technology Association. (2016). *Internet of things*: a framework for the next administration (white paper). Retrieved from <https://www.cta.tech/cta/media/policyImages/policyPDFs/CTA-Internet-of-Things-A-Framework-for-the-Next-Administration.pdf>.

Darmour, J. ([s.d.]) The internet of you: when wearable tech and the internet of things collide. *Artefact Group*. Retrieved from <https://www.artefactgroup.com/articles/the-internet-of-you-when-wearable-tech-and-the-internet-of-things-collide/>.

DATA IS GIVING rise to a new economy. (2017, May 6). *Economist*. Retrieved from <https://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy>.

Denham, E. (2017, July 4) Promoting privacy with innovation within the law (Speech). In 30TH ANNUAL CONFERENCE OF PRIVACY LAWS AND BUSINESS, Cambridge. Retrieved from <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/promoting-privacy-with-innovation-within-the-law/>.

Doneda, D. (2006). *Da privacidade à proteção de dados pessoais*. Rio de Janeiro, Brasil: Renovar.

Duhigg, C. (2012, February) How companies know your secrets. *The New York Times*. Retrieved from <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp>.

Fisher, D. (2016a, June 3). FTC warns of security and privacy risks in IoT devices. *On The Wire*. Retrieved from <http://www.onthewire.io/ftc-warns-of-security-and-privacy-risks-in-iot-devices/>.

_____. (2016b, October 13). The internet of dumb things. *Digital Guardian*. Retrieved from <https://digitalguardian.com/blog/internet-dumb-things>.

Ftc Staff Report. (2015). *Internet of things*: privacy & security in a connected world. [S.l.]: [s.n.]. Retrieved from <http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>.

Global Pulse (2012). *Big Data for Development*: Challenges and Opportunities. New York: [s.n.]. Retrieved from <http://www.unglobalpulse.org/sites/default/files/BigDataforDevelopment-GlobalPulseMay2012.pdf>.

Grassegger, H., & Krogerus, M. (2017, January 28). The data that turned the world upside down. *Motherboard*. Retrieved from <https://motherboard.vice.com/en_us/article/how-our-likes-helped-trump-win>.

Haupt, M. (2016). "Data is the New Oil"—A Ludicrous Proposition. *Medium*. Retrieved from <https://medium.com/twenty-one-hundred/data-is-the-new-oil-a-ludicrous-proposition-1d91bba4f294>.

Kuneva, M. (2009). Keynote Speech. *Roundtable on Online Data Collection, Targeting and Profiling*. Retrieved from <http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm>.

Landim, W. (2014, January). Wearables: será que esta moda pega? *Tec Mundo*. Retrieved from <http:/www.tecmundo.com.br/tecnologia/49699-wearables-sera-que-esta-moda-pega-.htm>.

Lane, J. et al. (Eds.). (2014). *Privacy, Big Data and the public good*: frameworks for engagement. New York, United States: Cambridge University Press.

Leonardi, M. (2011). *Tutela e Privacidade na Internet*. São Paulo, Brasil: Saraiva.

Macedo Júnior, R. (1999, January/December). Privacidade, Mercado e Informação. *Justitia*, São Paulo, *61*, 245-259.

Madden, M. (2012, February 24). Privacy management on social media sites. *Pew Research Center's Internet & American Life Project*. Retrieved from <http://www.isaca.org/Groups/Professional-English/privacy-data-protection/GroupDocuments/PIP_Privacy%20mgt%20on%20social%20media%20sites%20Feb%202012.pdf>.

Magrani, Eduardo. (2017). The Emergence of the Internet of Things. Internet Policy Review. HIIG, 2017.

_____. (2017, June). The emergence of the Internet of Anonymous Things (AnIoT). *Internet Policy Review – Journal on Internet Regulation*. Retrieved from <https://policyreview.info/articles/news/emergence-internet-anonymous-things-aniot/693>.

Mcdonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, *4*(3), 543-568.

Mcnulty, E. (2014, May 22). Understanding Big Data: the seven V's. *Dataconomy*. Retrieved from <http://dataconomy.com/2014/05/seven-vs-big-data/>.

Meola, A. (2016, December 19). How the internet of things will affect security & privacy. *Business Insider*. Retrieved from <http://www.businessinsider.com/internet-of-things-security-privacy-2016-8>.

Molaro, C. (2013, July 19). Do not ignore structured data in Big Data analytics: the important role of structured data when gleaning information from Big Data. *IBM Big Data & Analytics Hub*. Retrieved from <http://www.ibmbigdatahub.com/blog/do-not-ignore-structured-data-big-data-analytics>.

Moraes, M. C. B. (2013). Biografias não autorizadas: conflito entre a liberdade de expressão e a privacidade das pessoas humanas? Editorial. *Civilistica.com*, Rio de Janeiro, *2*(2), 1-4.

Mulholland, C. (2012). O direito de não saber como decorrência do direito à intimidade. *Civilistica.com*, Rio de Janeiro, *1*(1), 1-11.

Nascimento, R. (2015, March 12). O que, de fato, é internet das coisas e que revolução ela pode trazer? *Computerworld*. Retrieved from <http://computerworld.com.br/negocios/2015/03/12/o-que-de-fato-e-internet-das-coisas-e-que-revolucao-ela-pode-trazer/>.

O'Brien, C. (2016, August). Wearables: Samsung chases fitness fans with gear fit 2. *The Irish Times*. Retrieved from <http://www.irishtimes.com/business/technology/wearables-samsung-chases-fitness-fans-with-gear-fit-2-1.2763512>.

Obar, J. A., & Oeldorf-Hirsch, A. (2016). The biggest lie on the internet: ignoring the privacy policies and terms of service policies of social networking services. In: *The 44th Research Conference on Communication, Information and Internet Policy*. Retrieved from <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465>.

Oliveira, M. (2016, October). Em marketing, Big Data não é sobre dados, é sobre pessoas! *Exame*. Retrieved from <http://exame.abril.com.br/blog/relacionamento-antes-do-marketing/em-marketing-bigdata-nao-e-sobre-dados-e-sobre-pessoas/>.

Paiva, F. (2017, September). 'O modelo de consentimento falhou', diz professor da FGV. *Mobile Time*. Retrieved from <http://www.mobiletime.com.br/26/09/2017/-o-modelo-de-consentimento-falhou--diz-professor-da-fgv/477582/news.aspx>.

Palmer, Michael (2006, November). Data is the new oil. *ANA Marketing Maestros*. Retrieved from <http://ana.blogs.com/maestros/2006/11/data_is_the_new.html>.

Plouffe, J. (2016, December 23). The ghost of IoT yet to come: the internet of (insecure) things in 2017. *Mobile Iron*. Retrieved from <http://www.mobileiron.com/en/smartwork-blog/ghost-iot-yet-come-internet-insecure-things-2017>.

Poikola, A., Kuikkaniemi, K., & Honko, H. ([s.d.]). MyData – A Nordic Model for human-centered personal data management and processing. *Ministry of Transport and Communications*. Retrieved from <https://www.lvm.fi/documents/20181/859937/MyData-nordic-model/>.

Post, R. C. (2001). Three Concepts of Privacy. *Georgetown Law Review*, *89*, 2087-2098.

Redação. (2014, March). Parlamento Europeu reforça proteção dos dados pessoais dos cidadãos. *Parlamento Europeu*. Retrieved from <http://www.europarl.europa.eu/news/pt/press-room/20140307IPR38204/parlamento-europeu-reforca-protecao-dos-dados-pessoais-dos-cidadaos>.

Redação. (2012, February). Varejista norte-americana descobre até gravidez de clientes com a ajuda de software. *Olhar Digital*. Retrieved from <https://olhardigital.com.br/noticia/varejista-norte-americana-descobre-gravidez-de-clientes-com-a-ajuda-de-software/24231>.

Rijmenam, M. (2015, August). Why the 3 V's are not sufficient to describe Big Data. *DATAFLOQ*. Retrieved from <https://datafloq.com/read/3vs-sufficient-describe-big-data/166>.

Rodotà, S. (2008). *A vida na sociedade de vigilância* – a privacidade hoje. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro, Brasil: Renovar.

Rodrigues, A., & Santos, P. ([s.d.]). A ciência que faz você comprar mais. *Galileu*, [s.d.]. Retrieved from <http://revistagalileu.globo.com/Revista/Common/0,,EMI317687-17579,00-A+CIENCIA+QUE+FAZ+VOCE+COMPRAR+MAIS.html>.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*, 2266-2279.

Rose, K., Eldridge, S., & Chapin, L. (2015, October). The internet of things: an overview. Understanding the issues and challenges of a more connected world. *The Internet Society*. Retrieved from <http://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151022.pdf>.

Santos, M. W. (2017, March 16). O Big Data somos nós: a humanidade de nossos dados. *Jota*. Retrieved from <https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-big-data-somos-nos-a-humanidade-de-nossos-dados-16032017>.

Sarlet, I. W., Marinoni, L. G., & Mitidiero, D. (2012). *Curso de Direito Constitucional*. São Paulo, Brasil: Editora Revista dos Tribunais.

Sjöberg, M. et al. (2016). Digital Me: Controlling and Making Sense of My Digital Footprint. In: Gamberini, L. et al (Eds.). *Symbiotic Interaction*: Lecture notes in computer science (pp. 155-156). Padua, Italy: Springer.

Sloan, R. H., & Warner, R. (2014). *Unauthorized Access*: The Crisis in Online Privacy and Security. London, England & New York, United States: CRC Press.

Soprana, P. (2017, September). Internet das Coisas: Brasil lidera em disposição para fornecer dados pessoais. Época. Retrieved from <http://epoca.globo.com/tecnologia/experiencias-digitais/noticia/2017/09/internet-das-coisas-brasil-lidera-em-disposicao-para-fornecer-dados-pessoais.html>.

Venturini, J. et al. (2016). *Terms of Service and Human Rights*: an analysis of online platform contracts. Rio de Janeiro, Brasil: Revan.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193-220.

Weber, R. H. (2010). Internet of things: new security and privacy challenges. *Computer Law & Security Review*, *26*, 23-30.

20 Mi casa es su casa: The Impact of Digital Assistants on Privacy in Latin America

Luã Fergus Oliveira da Cruz

Abstract

This chapter aims at studying the possible threats that digital assistants can bring to Latin American users and consumers. This analysis was carried out through a bibliographic research on the recent implications related to the privacy provided by these products and applications, through the exploitation of sources that deal with the use of *big data* in the Global South and for the documentary analysis of patent applications, terms of use and Alexa privacy policies, used by the Echo family of devices, both developed by Amazon, currently the main digital assistant on the market. The study makes a forecast for a scenario in which such assistants are increasingly present in households in the region and, finally, aims measures *ex ante* to mitigate the possible harmful effects to privacy caused by these devices.

20.1 Introduction

The arrival of Internet of Things or Internet of Things (IoT), that is, the interconnection and connection to the Internet of physical objects, vehicles and other products in which sensors capable of collecting and transmitting data are incorporated, is considered one of the most disruptive changes of the current times, and promises to impact our lives in several ways. At the same time, this interactivity and interconnectivity presents considerable opportunities for technological development and challenges to privacy and the protection of personal data.

The products that today are integrated with the Internet of Things are from the most varied areas and have diverse functions, from household appliances to footwear, clothes, means of transport and even toys[395]. One product in particular draws attention in the international market and began to emerge on the Latin American shelves: the speakers that have a built-in personal voice assistant software.

395 See Hung (2016).

These virtual assistants use artificial intelligence techniques to analyze the requests of the users and return information, supposedly useful. They seek to become so natural that we will hardly perceive that they are hearing us all the time[396]. Every time an assistant records our voices, the sound files are sent and stored on the servers of the companies. Through the collection and analysis of *big data*, these assistants will process a large amount of information about us.

The IoT phenomenon is intimately connected to discourses about *big data*, whose optimistic versions envision many advantages for the general public, with the development of a more efficient society. But such a position must take into account the possible threats to the protection of privacy and in this context there are many areas that deserve greater care in terms of the impact of the IoT and *big data*, especially issues such as health, education, targeted marketing and access to services. This dose of skepticism derives from the announced capabilities of the tools that collect data in the field of IoT and use *big data*, because the feeding of the data bases and the techniques of processing and aggregation of data cause that the companies manage to draw models of behavior, establishing extremely detailed profiles that can expose personal and sensitive information until then unknown.

That said, this article aims to study the possible threats that the diffusion of the connected objects and, particularly, of the virtual assistants, can bring to the users and consumers of the Latin American region, realizing a forecast of a scenario in which such assistants are increasingly present in our Households.

This study will be carried out through a bibliographic research on the recent implications related to privacy provided by digital assistants through the exploration of sources that address the use of *big data* in the Global South and the documentary analysis of patent applications and Terms of Use and Privacy Policies of the main digital assistant of the market of the main domestic digital

396 "Amazon Echo uses a word recognition system on the device to detect a word conversation ("Alexa", "Echo", "Amazon "and" Computer "are standard conversations"). When these devices detect the voice conversation, they transmit the audio to the cloud, including a fraction of a second of audio before the *wake word*. [Author's translation]. See Alexa and Alexa Device FAQs. Available at: <http://amzn.to/2CmVZRP>.

assistant of the market, Alexa, used by the devices of the Echo family, both developed by Amazon.

20.2 Digital assistants, Amazon Echo and Alexa

Basically, a virtual assistant is software that can perform tasks or services for an individual. This device listens passively in order to identify keywords (said *hot word* or *wake word*) to activate. To do this, you must constantly listen and process the ambient sound, hoping to capture the activation word. When connected to other devices, attendees can also perform activities such as lowering the lights in the house, controlling the thermostat, connecting the sprayer and checking the electronic nanny.

One of these devices is the Amazon Echo (abbreviated and known as Echo) which is the wireless speaker developed by Amazon. The device uses the Alexa software, functioning as the physical extension of the assistants. In addition to voice interaction, it is possible to highlight other functions such as the ability to play music, make lists of tasks, configure alarms, transmit podcasts, play audiobooks and provide weather, traffic and other information in real time. The devices of the Echo family are also capable of controlling several devices functioning as a residential hub.

The choice of the Echo/Alexa duo as object of study is due to the fact that these Amazon products are dominant in the digital assistants market, with more than 30 million units sold[397] and a *market share* which varies between 70% and 76%, depending on the report[398].

As explained earlier, the products of the Echo family, as well as most digital assistants, work by hearing a "wake word." Once the voice conversation is pronounced, the Echo transitions from a passive hearing state to a responsive state. Amazon claims that it only stores and analyzes spoken audio after listening to the spoken word. Depending on the configuration of the device, in the passive

397 Voicebot. Amazon Echo & Alexa Stats. 2018. Available at: <https://www.voicebot.ai/amazon-echo-alexa-stats/>.

398 See Hao (2018).

listening state, Echo captures and analyzes all conversations that occur in the vicinity, but does not permanently register them or transmit them to their servers. As soon as the Echo detects that someone said the wake word, it enters into a responsive state, in which it records the subsequent audio and sends it to the Amazon servers for due processing[399]. It is in this situation that Amazon's natural language processing algorithms determine whether the user asked Alexa to, for example, darken the lights or order a pizza.

In addition to the functions officially disclosed by Amazon, a number of other possible applications for Alexa are also public knowledge. A recent study by Consumer Watchdog[400] revealed that Amazon filed patent applications for a number of technologies that would significantly extend the analytical capabilities and scope of monitoring the private lives of the users of such assistants. These applications for patent application show how technology companies use household data to draw conclusions about families and how they can use this data for financial gain.

Among the features described in Amazon's patent applications is, for example, an "audio processing algorithm" that analyzes the captured speech, which translates the audio to the text, when the device is in passive listening mode. Other patent applications mentioned in the study[401] refer to the systems that identify those who speak in a conversation and build profiles of interest for each one. These profiles can help the devices to adapt the services to the person speaking, and also to associate behaviors with individual members of the family, to better guide the announcements. There are also requests regarding systems for inserting paid content into the answers provided by the digital assistants.

It is important to emphasize that the fact that just because a company has applied for a patent does not mean that such a patent is developed or will be implemented. The patents, however, reflect the ambitions of a company.

399 See Alexa and Alexa Device FAQs. Available at: <http://amzn.to/2CmVZRP>.

400 See Consumer Watchdog (2017).

401 See Consumer Watchdog (2017: 8).

20.3 Terms of Use and Privacy Policies of Alexa

In addition to the study of patent applications, another interesting method to understand the objectives of the companies that develop electronic assistants is the analysis of the Terms of Use and the Privacy Policies. In this regard, it is worth highlighting the effective regulatory function of these documents that shows how contractual agreements have the potential to affect specifically the rights related to the privacy of users of technology products and services.

The methodology used for this evaluation is derived from that used in the study "Terms of Service and Human Rights"[402], developed by the Technology and Society Center of the Getulio Vargas Foundation, in association with the Council of Europe, which arose from the challenge of developing special parameters that could evaluate the adequacy of online platform documents in terms of human rights. Although the original methodology addressed a number of fundamental rights, the analysis developed in this chapter dealt only with the right to privacy, and in it the following activities related to user's personal data were verified: collection, retention, aggregation, use and protection before third parties.

Among the most significant results for this work, it was discovered that in terms of data collection, the documents make no mention of attempts to minimize the accumulation of collected data and are ambiguous when they address issues of user control over personal data available on the platform, either for the exclusion or alteration of the data provided. There is also no mention of data retention, that is, it is not possible to know if the platform retains the data for longer than necessary for the operation of the service offered.

Regarding the aggregation of data, the integration of data between different services and products of Amazon is expressed[403], and regarding its use, data are shared with a huge variety of third parties, justified by technical and commercial issues, but without more detailed information on such needs.

402 See Venturini et al. (2016: 20).

403 "The aggregation of data in various services or devices requires greater diligence on the part of the data controller, since it can result in data processing beyond the original purpose for which there was the collection and generation of new data, whose nature, Volume and meaning may not be known or known by the user of the platform."[Author's translation] (Venturini et al., 2016).

Finally, as regards protection before third parties, the transmission of data and content is encrypted, but they make no mention of the protection of data stored on the company's servers, and how the company shares data with the authorities when it "Believes that it is appropriate for compliance with the law", that is, only by reading the Terms of use it is not possible to affirm whether they require a citation, judicial or court order[404].

20.4 International expansion of the Echo / Alexa duo

It is important to remember that this work has as a geographical focus in the Latin American region and, for now, despite the launch announcements of Amazon Echo in some countries of Latin America (Chile, Colombia, Peru and Uruguay), the company has not yet extended Alexa services for any of the Romance languages spoken in the region, such as Spanish and Portuguese, or in other languages, such as French or Italian[405].

Despite the rapid growth of sales and all the interest created around Alexa/Echo, an area where the company chose not to rush is international expansion, and this activity has been well planned. At the beginning of 2017, both the service and the hardware were available only in the United States, the United Kingdom and Germany. Recently, they were also launched in India and Canada, giving Amazon access to a potentially huge customer base – and data base. At the end of 2017, company assistants arrived in Japan, a country known for adopting new technologies.

In executive interviews it is possible to notice the intentions of the company, which tries to prevent Alexa from sounding like a US product[406]. On the contrary, the company seems to want to convey the perception that the assistants as local products so that they can seduce potential consumers. However, such a strategy requires more time, because software needs to be developed with

404 Despite not being expressed in its documents, according to the report Who Has Your Back 2017, of the Electronic Frontier Foundation, the company adopts the best practices accepted by the industry, demanding a mandate to share content, publishing guidelines for the application of the law and publishing a transparency report. (EFF, 2017).

405 See Sewers (2017).

406 See Wadell (2016).

the ability to understand and pronounce colloquialisms, accents, places, names and streets, sounding as natural as possible.

The contextualization of the situation in which the expansion of Alexa occurs is very important for the critical position that this article assumes; however, the discussions about the so-called "surveillance capitalism"[407] are extensive in recent literature, in addition to being better explained and developed in other works, for this reason, they will not be studied in depth in this work.

The logic of surveillance capitalism, driven by the big technology companies, is based on intensified patrolling of its users, and consequently, on the exploitation of users' personal data by creating detailed profiles of the public with the final objective of expanding and making it easier to market products. Thus, some experts[408] assert that there is a transfer of work from the company to users and consumers, once they work producing data, but without remuneration, being, therefore, considered as "digital slaves"[409].

20.5 Latin America: data producer instead of technology

The use of connected products traced in environments of *big data* is something present in the daily life of most of the inhabitants of Latin America, but Latin Americans are still only consumers of these major technologies, and not developers or suppliers, although we have examples of technological successes in the region. This observation leads to speculation that these technologies are developed without taking into account our local and regional needs.

Another concern related to the use of *big data* is for its ability to reproduce the biases and preconceptions contained in the data provided by the users themselves, becoming a tool for perpetuating and strengthening the economic and social discomfort experienced by the countries of our region. In addition, it is important to remember that some countries still do not have a general law for the protection of personal data, such as Brazil and Paraguay, which

407 This expression defines a new form of capitalism that aims to anticipate, modify and manipulate human behavior, based on data collection. See Zuboff (2015).

408 See Vieira & Evangelista (2015).

409 See Belli (2017).

facilitates potentially abusive practices, carried out both by the private sector, seeking profit, and by governments, seeking greater political power through control and surveillance measures.

In this way, although assistants, applications, platforms and other connected objects are common to citizens around the world, it is necessary to analyze the implementation of these devices through specific parameters of each region, as is the case in Latin America.

A curious element to keep in mind in this discussion is the profile of the Latin American user. A global survey[410] that counted on the participation of four Latin American countries (Brazil, Argentina, Colombia and Mexico), identified that the majority of the inhabitants of these countries support the use of Internet-connected devices for emergency alerts, baggage tracking, and means of payment and monitoring of the Health. Colombia presented a great approval of these initiatives (91%), the largest among the countries of Latin America, followed by Brazil (88%), Mexico (86%) and Argentina (81%). The profile of *early adopter* of Latin Americans is one of the explanations for the support and enthusiasm with these new devices.

Although the use of personal data by software is associated with a relevant interest for local users, the fact is that this procedure raises several data protection issues, especially when both the incentive and expectations are being created by consumers in the region.

20.6 Perspectives and suggestions

An ex ante approach in relation to the future conjuncture outlined in the work has the capacity to ensure certain preconditions to promote greater privacy protection, ensuring that the incentives of the services are aligned with the interests of the users and causing certain dynamics to be avoided of the market that may give rise to exclusion or exploitation effects.

During the elaboration of this article, with the help of the bibliography that deals with the topic, some technical alternatives and regulatory recommendations emerged to minimize the negative impacts of these new tools in relation to the user's right to privacy. Some recited measures will be presented: technical developments, alterations

410 See Unisys (2017).

in the hardware, informative notifications to the users, respect to the principles of the concept *privacy by design / by default* and improvement in the wording of the terms of use.

20.6.1 Powerful processors

Echo needs to be connected to the Internet to function, since attendees are still not "smart" enough to do all the necessary work on their own, they need to delegate to the remote servers the realization of "heavy work", and that is precisely why the privacy issues arise, since there is a huge amount of traffic and data storage every time they try to answer a question.

However, this scenario tends to change, since the processors of these devices have become increasingly powerful, that is, the prospect of an assistant who lives completely on their hardware will be executable[411].

An internal Artificial Intelligence (AI) would allow a digital assistant to perform some tasks without the need to connect to the Internet. Even when the assistant needed the Internet to respond to a request, the local AI could perform all the voice analysis and decoding on the device itself, sending only one final question, in an encrypted and anonymous form. Only when the devices manage to work that way, becoming independent, will they really be discreet and harmless assistants. However, technology companies have their main source of profit in data processing, so this future scenario of powerful chips in household appliances should not be taken as a guaranteed future.

Voice assistants still depend on Internet access, and while the processor technology is not up to our needs it is necessary to think of solutions that can mitigate current problems more immediately.

20.6.2 Well-informed users

In a *paper*[412] regarding the case of devices controlled by voice commands, the Future of Privacy Forum suggests some good practices for the manufacturers of these types of products,

411 For more details on the technical performance of this new chip model see Sze, Yang, Chen & Emer, (2017).

412 See Gray (2016).

among the recommendations: a) Greater transparency in the transmission of voice data to the servers of the company; b) Notice clearly informed to the user about important privacy issues before installation of the device; c) Need for an on / off switch that can deactivate the microphone; and d) the provision of visual indications that clearly demonstrate when the apparatus is recording and / or transmitting information.

Well-informed knowledge and voluntary consent are fundamental, since many times the current way of obtaining consent is illusory, since the terms and conditions are practically imposed on users. The simplest measures are some of the solutions indicated by the authors[413] to guarantee certain autonomy to users, such as the insertion of clear indications that a product is being offered to the detriment of another for commercial reasons and the ability to choose not to receive personalized advertisements or sponsored products.

20.6.3 Privacy by design

The concept of privacy *by design* was created in 1990 by Ann Cavoukian[414] to refer to a privacy approach that is directly incorporated into the technological structures developed, the business models and the infrastructures used by them.

The notions of privacy by design and privacy by default require a commitment to strengthen the scope of protection of personal data and is associated with the idea that privacy is advantageous not only for the users, but also for the private sector, since the construction of protective mechanisms from the beginning has the capacity to produce many gains derived from the reinforcement of trust.

This is an interesting concept, since it divides the responsibility on the subject also to other levels, such as the elaboration of software and protocols, the construction of physical infrastructures (hardware), in addition to the platforms of the content layer, so that the protection of personal data is incorporated in all areas.

413 See Stucke & Ezrachi (2017).

414 See Cavoukian (2011).

20.6.4 Improvement of Terms of Use

The importance of the role played by the services offered by the Internet is well known and, in order to continue their activities, technology companies set up uniform rules in several jurisdictions. It is understood that this mechanism of application of private norms is in agreement with the dynamic nature of the Internet. Thus, it is often concluded that these companies play the role of regulators because of their ability to stipulate and apply the rules of their services[415].

However, given the analysis of Alexa's Terms of Use and Privacy Policy, it is necessary to think of measures that companies can take to ensure that their users are not subject to unnecessary collection, aggregation, use and disclosure of users' personal data. Therefore, setting minimum standards and developing voluntary practices at the national and regional levels to ensure the protection of human rights by transnational corporations becomes a non-expendable task.

Some initiatives within the framework of the United Nations are already moving forward in this regard, such as the Recommendations on Terms of Use and Human Rights developed by the Dynamic Coalition on Platform Responsibility of the Internet Governance Forum (IGF), the United Nations Guiding Principles on Business and Human Rights[416], and also the opinion[417] of the special rapporteur for the promotion and protection of the right to freedom of opinion and expression.

20.7 Final Considerations

At the moment, Latin America is out of Alexa's reach, which may mean something negative, because we do not have at our disposal the immense range of activities that it can perform to improve our quality of life. But that also has its positive side, because we are still immune to the avalanche of problems related to the privacy that it can cause.

415 See Belli & Venturini (2016).

416 See UN (2011).

417 See Freedom of Opinion and Expression – Annual reports. Available at: <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx>.

The integration of voice recognition in our lives will offer a series of benefits for the comfort of users' day to day, but it will also bring concerns to the protection of privacy. However, it is important to recognize that voice has been an increasingly useful interface to get involved with our devices, due to its communicative content, and we will need to advance in the protection of these biometric data. The increasing prevalence of voice as the main way to interact with devices allows companies that develop and implement voice interfaces to collect, store and analyze huge amounts of personal data. However, users do not always understand when and in what way these devices are collecting information, so it is imperative to think and discuss appropriate legal and technical guarantees as digital assistants become popular.

The fact that digital assistants are not yet present in Latin American houses presents a great window of opportunity to prepare us efficiently in regard to the protection of fundamental rights such as the protection of privacy, intimate life, inviolability of the home, among others. The suggestions and measures presented in this article are not exhaustive and should be complemented with further analyzes based on concrete evidence. But we should not adopt such an optimistic position, since the debate on personal data protection in many countries of the region is outdated, delayed and broken with the current scenario of technological innovations.

It is necessary to ensure that the public clearly understands the risks that can be linked to the use of connected devices and, particularly, when these devices can record personal conversations, and how the information obtained can be used. The exchange of privacy for convenience is generally considered acceptable by users, but that exchange must be well informed.

That said, the State, the companies and the citizens that make up this scenario must be attentive to the challenges that lie ahead. Legislators and other members of the public power must seek to establish legal parameters that promote the protection of personal data and the privacy of citizens in an individual and collective approach. Technology companies need to take responsibility for the immense control they exercise over consumers, and for this it is desirable that they align with the principles, regulations and

best practices established to guarantee respect for positive human rights in national and international documents. Finally, it is up to the citizens to be attentive to the power that exists in the handling of personal data by companies, and also be aware of the subsequent consequences for welfare, privacy and other fundamental rights.

20.8 References

Belli, L. & Venturini, J. (2016). Private ordering and the rise of terms of service as cyber-regulation. Internet Policy Review, 5(4). DOI: 10.14763/2016.4.441. <https://policyreview.info/articles/analysis/private-ordering-and-rise-terms-service-cyber-regulation>.

Belli, L. (2017). Os dados pessoais e os escravos digitais. Nexo Jornal. <https://www.nexojornal.com.br/ensaio/2017/Os-dados-pessoais-e-os-escravos-digitais>.

Cavoukian, A. (2011). Privacy by Design – The 7 Foundational Principles. <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>.

Consumer Watchdog (2017). Google, Amazon Patent Filings Reveal Digital Home Assistant Privacy Problems. <http://www.consumerwatchdog.org/sites/default/files/2017-12/Digital%20Assistants%20and%20Privacy.pdf>.

Electronic Frontier Foundation (2017). Who Has Your Back? Government Data Requests 2017. <https://www.eff.org/files/2017/07/08/whohasyourback_2017.pdf>.

Future of Privacy Forum (2016). Always On: Privacy Implications of Microphone-Enabled Devices. <https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf>.

Hao, K. (2018, 8 de janeiro). Amazon Echo's dominance in the smart-speaker market is a lesson on the virtue of being first. Quartz. <https://qz.com/1157619/amazon-echos-dominance-in-the-smart-speaker-market-is-a-lesson-on-the-virtue-of-being-first/>.

Hung, Mark (2017). Leading the IoT – Gartner Insights on How to Lead in a Connected World. <https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf>.

IGF (2015). Recommendations on Terms of Service and Human Rights. Presented at the 10th United Nations Internet Governance Forum. <http://www.intgovforum.org/cms/documents/igf-meeting/igf-2016/830-dcpr-2015-output-document-1/file>.

Mitchell, S. (2017, 25 de junho). Amazon Is Trying to Control the Underlying Infrastructure of Our Economy. Motherboard. <https://motherboard.vice.com/en_us/article/7xpgvx/amazons-is-trying-to-control-the-underlying-infrastructure-of-our-economy>.

ONU (2011). Guiding Principles on Business and Human Rights. <http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf>

Rogers, EM (1962). Diffusion of Innovations. Free Press of Glencoe, Macmillan Company. <https://teddykw2.files.wordpress.com/2012/07/everett-m-rogers-diffusion-of-innovations.pdf>.

Sawers, P. (2017, 08 de dezembro). Amazon Echo speakers arrive in 80 new markets, as Amazon Music Unlimited expands across Europe and Latin America. Venture Beat. <https://venturebeat.com/2017/12/08/amazon-music-unlimited-expands-to-28-new-markets-in-europe-and-latin-america/>.

Stucke, ME & Ezrachi, A. (2017). How Your Digital Helper May Undermine Your Welfare, and Our Democracy. Berkeley Technology Law Journal, Forthcoming; University of Tennessee Legal Studies Research Paper No. 324. <https://ssrn.com/abstract=2957960>.

Sze, V., Chen, Y., Yang, T & Emer, J. (2017). Efficient Processing of Deep Neural Networks: A Tutorial and Survey. <https://arxiv.org/pdf/1703.09039>.

The Capital Forum (2016). Amazon: By Prioritizing its Own Fashion Label Brands in Product Placement on its Increasingly Dominant Platform, Amazon Risks Antitrust Enforcement by a Trump Administration. <https://thecapitolforum.com/wp-content/uploads/2016/07/Amazon-2016.12.13.pdf>.

Unisys (2017). Unisys Security Index Global 2017. <http://www.app5.unisys.com/library/cmsmail/USI/Unisys%20Security%20Index_Global.pdf>.

Upstream Commerce (2014). Does Amazon Eye Its Own Marketplace Vendors' Best Sellers? <http://upstreamcommerce.com/blog/2014/10/28/amazon-muscles-marketplace-vendors-sellers>.

Venturini et al. (2016). Terms of Service and Human Rights: an Analysis of Online Platform Contracts. <http://internet-governance.fgv.br/sites/internet-governance.fgv.br/files/publicacoes/terms_of_services_06_12_2016.pdf>.

Vieira, MS e Evangelista, R. A máquina de exploração mercantil da privacidade e suas conexões sociais (2015). 3rd International LAVITS Symposium, Rio de Janeiro, 2015. <https://ssrn.com/abstract=2608251>.

Wadell, K. (2016, 24 de maio). The Privacy Problem with Digital Assistants. The Atlantic. <https://www.theatlantic.com/technology/archive/2016/05/the-privacy-problem-with-digital-assistants/483950/>.

Zuboff, S. (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. Journal of Information Technology (2015) 30, 75–89. <https://doi:10.1057/jit.2015.5>.

21 The Right to Be Forgotten in Brazilian Justice in the Era of the "Fake News"

Cláudio Soares Lopes

Abstract

The constant growth of the number of Brazilians connected to the Internet, the proximity of the elections, and the emergence of the debate on *fake news*, is located at this juncture that this chapter intends to address in relation to the right to be forgotten and its possible interpretations in the Brazilian Justice. Taking into consideration the dictatorial past and the recent Brazilian democracy, and through the analysis of the current Brazilian legal system, the recent decisions dictated by the high courts and the best doctrinal understandings, this work has the purpose of presenting the diverse existing interpretations on the recognition to the oblivion of past facts, presenting which ways and solutions will be able to be followed in the next judgments of the Federal Supreme Court.

21.1 Introduction

In the modern world, no one doubts the importance of what the Internet represents as a tool for humanity. It would be unimaginable to think of present day life without this fundamental mechanism of social development.

Just to mention a fact of what is happening in Brazil, for a population of almost 207 million people, there are approximately more than 300 million mobile devices in circulation. That is almost an average of 1.5 devices per inhabitant[418].

Obviously, almost all these devices have the possibility of accessing the internet. Therefore, in a still poor country, with great social inequality and, at the same time, admittedly one of the largest world economies, it can be said that at least 60% of the population is partially "connected". Therefore, tens of millions of Brazilians of all classes have access to the global network of computers, and

418 See IBGE (2017).

everything that is disclosed and circulated through it, despite the existence of Internet regulation, enshrined in the Civil Framework of Internet – Law No. 12.965 / 2014 – and in the Decree No. 771 / 2016 that regulates this norm.

It is evident that this reality has transformed the relations between people and, especially, the life of the political class, giving rise to the discussion of how to combat the so-called "fake news", that is, false or untruthful news that could influence the electoral debates transmitted in the social networks and groups of WhatsApp — this on the eve of the next and very important general elections that are going to take place in October 2018, mainly in the absence of legislative regulation in the Brazilian law on the subject.

Many jurists, politicians and members of the electoral justice are working towards the creation of measures to minimize the harmful effects of these practices on the outcome of the polls.

And it is in this context that we can introduce a sensitive issue, which is the confrontation with the recognition of the right to "forget" facts and news circulating on the Internet and other media.

Could it be that after some period, after a few years, people mentioned in journalistic materials referring to facts that involve them although true, could request the de-indexing of the information and images associated with their names in published results on search sites?

And should the criteria to assess the relevance of these materials be the same when such news refers to a public figure, as politicians, or when referring to "ordinary" citizens?

21.2 Brazilian legislation

Brazilian law, strictly speaking, does not specifically deal with this issue, that is, the right to be forgotten, at least clearly. There is the need to combine a series of constitutional norms and infra constitutional laws and jurisprudential interpretation, in order to try to build a solution, case by case.

In effect, the Brazilian Law guarantees, as an individual guarantee, the right to privacy, privacy and human dignity, on the one hand, and the right to freedom of expression, prohibiting censorship, on

the other, as it is extracted from articles 1, III, 4, II, 5, IV, IX, X and XIV, 220, 221 and 222, § 3.

On the other hand, in Law 12.965, of April 23, 2014, known as the Internet Civil Framework in Brazil, there are no specific rules regarding the subject. The aforementioned law, in accordance with the Federal Constitution, basically ensures the same principles listed above, which can be observed in various provisions.

In particular, we can highlight articles 2, II, 3, I and II, 7, I, 8, 10 and 19, in which there is always an allusion to respect for freedom of expression on the one hand and protection of the privacy and the inviolability of the privacy of private life, on the other.

Article 19 draws attention, by providing:

> Article 19. In order to ensure freedom of expression and prevent censorship, the Internet application provider may only be held civilly liable for damages arising from content generated by third parties if, after the specific court order, it does not take measures to framework and in the technical limits of its service and within the indicated period, make available the content indicated as infringing, except for legal provisions to the contrary.
>
> § 1 The judicial order addressed in the introduction must contain, under penalty of nullity, clear and specific identification of the content indicated as infringing, which allows the unambiguous location of the material.
>
> § 2 The application of the provisions of this article for infractions of copyright or related rights depends on a specific legal provision, which shall respect the freedom of expression and other guarantees provided for in art. 5 of the Federal Constitution.
>
> § 3 The causes that refer to the compensation for damages derived from content available on the Internet related to honor, reputation or personality rights, as well as the non-availability of these contents by Internet application providers, may be presented in special lawsuits.

> § 4 The judge, even in the procedure provided for in § 3, may fully or partially anticipate the effects of the protection sought in the initial request, there being unequivocal proof of the fact and considered the interest of the community in the availability of content on the Internet, provided that the requirements of credibility of the author's allegation and well-founded fear of irreparable damage or of difficult repair.

Therefore, it is noted that there is a legal provision that the interested party may go to court to request the non-disclosure of news or images that may harm their honor and dignity, without mentioning a specific rule that takes care of the right to forget news or previous facts.

Law 8443/17, which seeks to create specific rules that "enable society to use faster mechanisms of protection and defense against those who practice criminal unlawful acts," is being processed in the National Congress, enabling the citizen to directly request the mass media or service provider to remove data that is offensive to their reputation.

The mechanism will examine, according to the project, the viability of withdrawing the news and, in case of divergence, it will be up to the judiciary to present a solution. The bill prohibits politicians and political agents from using the benefit.

Once again, however, we do not see a clear solution to the right to be forgotten.

We can also mention rules foreseen in the Brazilian legislation, whether in the Civil, Penal or Consumer Codes, which, in some way, they bring to collation, indicative that seek to protect the citizen from the disclosure of facts concerning privacy and privacy, without forgetting the guarantee of the rights of expression and manifestation, as is the case of articles 11, 20 and 21 of the Civil Code of 2002. The civil law in the aforementioned devices provides for the prohibition of disclosure of writings and images that achieve honor, fame, etc.

It is true that the Federal Supreme Court, in the ADI 4815, determined an interpretation according to the Constitution of articles 20 and

21 of the Civil Code, in order to avoid prior censorship in writings and publications.

On the other side, in the Civil Law Conference promoted by the Federal Justice Court / STJ, the question was explicitly raised in relation to the right to be forgotten, which, obviously, can only be conceived as a form of doctrinal interpretation, be deliberate the following:

> "STATEMENTE 531 – The protection of human dignity in society includes the right to be forgotten.
>
> Article: 11 of the Civil Code
>
> Justification: The damages caused by the new information technologies have been accumulating in the current days. The right to be forgotten has its historical origin in the field of criminal convictions. It emerges as an important part of the right of the former detainee to re-socialization. It does not attribute to anyone the right to erase facts or rewrite history itself, but only ensures the possibility of discussing the use given to past events, more specifically the manner and purpose with which they are remembered.
>
> Articles 93 of the Criminal Code and 748 of the Brazilian criminal procedure law ensure the right to the convicted person rehabilitated, after serving the sentence, to the secrecy of the records of the criminal process. In the same way, the Law of Criminal Executions.

21.3 Positions and concrete cases. From the Brazilian Federal Supreme Court to the Court of Justice of the European Union

What can be observed is that, strictly speaking, we can glimpse three doctrinal options regarding the possibility of recognition of the right to oblivion, which we intend to demonstrate in the following paragraphs. In Brazil, the question regarding the right to be forgotten is already being evaluated by the High Supreme Court in Extraordinary Appeal 833.248. On the other hand, the other ministers, by majority, knew how to attribute general

repercussion to the matter, due to the constitutional nature and the high relevance of the matter for society and for the media, so that, after the trial, the result will link to the other instances.

The question is so delicate and of public interest that the Minister Dias Toffoli, rapporteur of the aforementioned appeal, held a public hearing, seeking consensus.

The specific hypothesis in court refers to the interest of relatives, in the famous Aida Curi case. The hypothesis, in fact, does not refer to a situation of forgetfulness that implies some Internet search site. However, the basic issue, of general interest, is the one that presents a connection with the subject matter.

In the trial hypothesis, the living brothers of Aida Curi, brutally murdered in 1958, questioned the production of a television program that revived the crime to which she had been a victim. The objective claim was compensation for moral damages, because of reopened wounds, to the extent that the transmission of life, death and post-death of the late sister brought back to light the pain of a family tragedy already forgotten by the action of time.

In the first instance and in the headquarters of Special Appeal and judged in the Superior Court of Justice, the right to compensation was not recognized. However, now, the Brazilian Constitutional Court will face the issue, giving general repercussion to the court as indicated above, and the central issue on which a positioning is expected, especially before the absence of specific rules in Brazilian legislation. As it is demonstrated, it refers to the recognition or not, to the right to be forgotten, in the sense of non-reproduction in the media and Internet search sites references to past events that may cause some type of damage.

It is important to mention the opinion of the Attorney General's Office regarding the disproportion of the SR in question, on the grounds that there can be no exception to the right to information and disclosure of historical facts of interest to the community.

Three doctrinal currents can be admitted, in principle, with respect to the subject and that may be object of jurisprudential option. In the first place, we can recognize a current that does not admit a

right to be forgotten, due to a lack of legal provision and because it is not possible to imply any violation of the rights to privacy.

It is stated that freedom of expression is what should prevail. Even the recent decision of the Federal Supreme Court regarding unauthorized biographies in which the right to prior censorship was not recognized, as mentioned above, is invoked.

In addition, the right to be forgotten would be something that would be of interests to the memory of a people and their own history.

On the other hand, we find opinions totally in favor of the recognition of a broad right to be forgotten, as a corollary of the rights of the human person to privacy and dignity, principles that must prevail in relation to freedom of communication and information related to past events.

This would avoid labeling individuals, condemning them to perpetual penalties, to the extent that, even after serving their sentences, they would be subjected many years later to a public trial even by generations that were not even alive at the time of the events.

Some even propose a deadline for the press and Internet search sites to suppress any information after serving the sentence.

In the case that the right to forget has been recognized, it is even invoked, judged by the Superior Court of Justice (REsp 1334.097 / RJ) "Occurring in the early 90's, what was alluded to as "a right not to be remembered against your will". It should be noted that such an interpretation does not refer exclusively to the digital environment but, on the contrary, is much broader and applies to all media.

The intermediate position, and that we think may prevail in our maximum court is in the sense that there really does not exist, a priori, a hierarchy between the principles that guard the freedom of information and privacy.

We cannot forget that both are considered principles and recognized as fundamental rights. For this reason, we believe that it will depend a lot on the analysis of the specific case before the weighing of the legal assets and principles in conflict.

Thus, cases referring to politicians and public agents, the previous fame of victims who had other public projections, as was the case of the brutal crime involving the young actress of the TV Globo Daniella Peres by her colleague who caused enormous national commotion, the suicide of President Getúlio Vargas, the assassination of JFK, notorious and historic trials (such as the impeachment of President Fernando Collor de Melo), crimes practiced in times of dictatorships and wars, etc., will certainly not be recognized as apt to be "erased" from the memory of the general public.

In support of this intermediate position, we find relevant the trial of the Court of Justice of the European Union in the case of the request of the Spanish lawyer Mário Costeja González. The favorable ruling has generated a cause, forcing the Google search site to delete the registration of their personal data, as well as links to news from the newspaper La Vanguardia, referring to the call of the Ministry of Labor to an auction of real estate that occurred in 1998 to settle debts of his company.

It is appropriate to highlight that the previous decision did not determine that the newspaper's page be removed from the internet, but only the link to the newspaper's page. It is clear that Google, as well like any other search engine operating in the European Union, in order to respond to this decision, offered a form, with the objective that interested parties could request the removal of obsolete information and damaging news to their reputations.

It is verified, therefore, that the aforementioned judgment expressly accepted the recognition of the right to "be forgotten" in a specific situation.

21.4 Conclusion

The Brazilian law lacks of a specific legislation that takes care of the question regarding the right of recognition to the oblivion of past events, fitting, at the moment, a jurisprudential interpretation in concrete cases, which we hope will happen, shortly, by the Federal Supreme Court, bringing guidelines that can guide the right operators.

Although it adhered to the opinion expressed by some that there is not in principle a hierarchy between constitutional principles and, recognizing as fundamental, as a rule, the right to integral information, in the public interest for knowledge of the historicity of certain facts, we cannot fail to consider that the right to privacy and intimacy must prevail in some special cases.

It is essential that the exception to the publicity of certain facts, do not find support in historical facts that involve crimes committed, for example, in periods of dictatorships, tyrannies and wars, or the possibility of the public to have access to essential information to form their opinion about public officials who cover or want to fill elective positions.

In general, these crimes are prescribed or have been subject to amnesty, so that there is no possibility for the time course of application of criminal sanctions, so that interest in criminal compensation is usually harmed.

What cannot be admitted is that eventual agents who participated in these criminal acts or their relatives can request in justice the "forgetfulness" of those historical facts and find protection in a possible future law.

These facts should never be forgotten or erased from everyone's memory. On the contrary, they must be remembered to prevent dictatorships from being installed again, affecting the democracy that must prevail.

In the event that the Federal Supreme Court can appreciate the punishment to which it attributed general repercussion, establishing parameters, rules and limits, so that it can recognize the right to forgetfulness, at least in some cases where there is evident affectation of private interest, moving away from this possibility situations that are of public interest or knowledge, without prejudice, of the existing law, the Brazilian legislator comes to regulate and discipline the subject within the scope of its constitutional attributions, in order to guarantee legal security and better explanation of rights and duties.

21.5 References

IBGE. (2016). Pesquisa Nacional por Amostra de Domicílios. <https://agenciadenoticias.ibge.gov.br/busca-avancada.html?produto=9173>.

Superior Tribunal de Justiça (REsp 1334.097/RJ) <https://www.conjur.com.br/dl/direito-esquecimento-acordao-stj.pdf>.

Tribunal de Justicia de la Unión Europea (C-131/12) Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González. <http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:62012CJ0131>.

22 Challenges in Obtaining Evidence in Cybercrimes in Brazil: WhatsApp Case

Vanessa Fusco N Simões and *Hugo Fusco N Simões*

Abstract

The Brazilian population is increasingly using the Internet, both through smartphones and computers. Recent data shows that this access through smartphones (e-mobile) is preferred among users mainly to access social networks, mobile banking and transportation apps, and for online purchases. The increase in digital inclusion seen in the last ten years in Brazil also brings the migration of criminals to the virtual world. However, the Brazilian criminal and procedural legislation did not follow the speed of Internet access, and investigation and prosecution of a criminal who committed a cybercrime is currently a tough task for law enforcement, prosecutors and judges. Doctrine and jurisprudence, technicians and jurists debate the issue. However, meanwhile, more and more crimes occur without punishment in the virtual world in Brazil.

22.1 Introduction

In fact, half of the Brazilian population in 2017 has Internet access. There are more than 100 million people connected, especially nowadays through smartphones. Online devices have become the main option to communicate, make purchases, use Internet banking, obtain documents, transport applications, etcc ... However, this massive use of the Internet has also attracted criminals to this environment and the Brazilian´s hackers are internationally known for their creativity and, unfortunately, for impunity.

In fact, Brazilian legislation has not accompanied the evolution of the technologies and means of Internet access. Very slowly laws are being passed that refer to the subject, but the mechanisms of production of evidence are not yet sufficient for effective criminal prosecution and aren't even criminal offenses.

It should be noted that since 2001, the Budapest Convention has been in effect among the countries of the Council of Europe and has

been signed by the United States and Mexico[419]. This international instrument contains the standards that must be observed by the signatory States related to criminal law and criminal procedure in the field of cybercrimes. However, Brazil, after a long process of evaluation by a Working Group established in the Ministry of Foreign Affairs (or Itamaraty), in 2010 decided not to adhere to the aforementioned Convention and, as we will see in this article, the Brazilian decision has brought to the present day consequences with reflections in the criminal prosecution – specifically in relation to the weakness in the production of the evidence, in reference to the cybercrimes that have occurred in the country.

It is known that the Internet knows no borders. Therefore, it is to be imagined that one of the central issues in the criminal procedure field, related to cybercrimes, is international legal cooperation. First, because application providers, who have the data for a cybercrime, are likely to have their data centers outside Brazil and, therefore, cannot provide such information to the authorities without the use of international cooperation mechanisms. However, when dealing with international legal cooperation in criminal matters, in addition to the existence of the "rogatory-letter" order, Brazil has at its disposal several bilateral treaties of international legal cooperation in criminal matters with the United States and several other states, as MLAT (Mutual Legal Assistance Treaty). The Agreement on Judicial Assistance in Criminal Matters between the Government of the Federative Republic of Brazil and the Government of the United States of America was introduced into Brazilian legislation through Decree No. 3,810 of May 2, 2001 when access to the Internet in Brazil was still incipient.

After 16 years since its introduction in the national regulations, it needs an urgent improvement to adapt to the need for the agile production of the evidence in the virtual world. And as a mechanism to search the evidence outside of Brazilian jurisdiction, it has proven inefficient.

419 View <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=h3KHAGQW>.

This article aims to bring to the discussion the challenges faced by the actors of the justice system: Police, Public Ministry and the Judiciary, in what refers to the production of evidence in the Criminal Action in which it is sought in the condemnation of a cybercrime.

For this, the approach will start from the analysis of the conceptualization of what is understood by cybercrime and the means that are necessary to produce evidence in this field, besides bringing to light the doctrine and jurisprudence on the production of criminal evidence, in the specific case of the WhatsApp message exchange application.

22.2 Cybercrimes and criminal evidence

Criminal evidence can be defined, according to Fernando Capez, as originated from Latin ***probatio***, being the set of acts practiced by the parties, by the judge and by third parties, destined to take to the magistrate the conviction about the existence or nonexistence of a fact, of the falsehood or veracity of an affirmation. It is, therefore, all means of perception used by man in order to verify the truth of a claim. It is described in articles 156, part 2, 209 and 234 of the Criminal Process Code[420].

It is important to emphasize, however, that in order to carry out an investigation in the virtual environment, the investigator must prepare to develop his work in an environment with totally different characteristics: a volatile crime scene and one that is accessed only through technology, and that the elements of proof are, in most of the times, in the power of the private initiative. These evidence are popularly called digital traces, or technically, connection data or access logs.

First of all, one has to conceptualize what are data records, numbers or IP addresses (Internet Protocol) and the address of the computer or MAC address (*Media Access Control*).

Access logs is an expression used to describe the process of recording relevant events in a computer system. This record can be used to restore the original state of a system or for an administrator

420 View <http://programadeapoioaoestudantededireito.blogspot.com.br/2008/10/conceito-de-prova.html>.

to know its behavior in the past. A log file can be used to audit and diagnose problems in computer systems[421].

Internet Protocol in turn is an identification of a device (computer, printer etc.) in a local or public network. Each computer connected to the Internet has a unique IP address (*Internet Protocol* or Internet protocol), which is the medium which machines use to communicate on the Internet[422].

MAC address is a physical address associated with the communication interface, which connects a device to the network. The MAC is a "unique" address, meaning there are no two ports with the same numbering, it is used for access control in computer networks. Your identification is recorded in hardware, that is, in the RAM of the network card of equipment such as desktops, notebooks, routers, smartphones, tablets and network printers[423].

Each computer, cell phone, tablet, or any device connected to an Internet network, such as an Xbox or PS4 console, receives a unique number at the time of connection: the IP address. This IP is assigned to one of these devices to have a network connection, which the user had to contract (with the connection provider), be it mobile telephony or broadband. This IP address is, in general, dynamic, that is, it is assigned to each user only for the necessary time of their connection, being assigned again to another user as soon as that first connection ceases, and so on.

In this way, the records referred to above have to be provided by the connection providers with the exact time, with minutes and seconds and even with the time zone in which it was collected.

Only in this way is it possible to know which device was accessed through a user's account at that precise moment.

But how does one obtain such an "IP address" to use in a criminal investigation? The problems for the investigator begin there. The data that the authorities need invariably, as mentioned above, are held by the private initiative and can still be stored outside the country. Then things get complicated.

421 See <https://pt.wikipedia.org/wiki/Log_de_dados>.

422 See <https://pt.wikipedia.org/wiki/Endere%C3%A7o_IP>.

423 See <https://pt.wikipedia.org/wiki/Endereço_MAC>.

But are these data really preserved by the providers, both of connection and application providers? And how does one obtain them? Is there already an efficient mechanism? In the following lines we will talk concretely about the challenges in obtaining evidence in cybercrimes.

22.3 Challenges in the production of evidences in Brazil

The need to obtain evidence that is in the power of private initiative, connection and content providers, has been debated for a long time in Brazil. In Bill No. 84/1999, popularly known as the Azeredo Project, then a Federal Legislator, already envisaged a device, in an attempt to command the storage of data, establishing a deadline for it by suppliers, as well as defining cybercrime behaviors. However, after a long and noisy process, PL 84/99 became a far cry from its original form: it was enacted as Law No. 12.735 / 2012, with just one article. Only with the advent of the Internet Civil Framework (Marco Civil da Internet) the term for storage of connection and application usage logs by respective providers in Brazil was defined.

22.4 Regulatory framework in relation to data storage

The Law No. 12.965, of April 23, 2014, establishes duties, rights and principles to be respected for the use of the Internet in Brazil. It is more popularly called Internet Civil Framework (Marco Civil da Internet)[424]. This legal provision disciplined, among others, the data storage, which are merely the evidence that the criminal system operators need to instruct an investigation in the virtual environment, which in turn will base the offer of a complaint.

Article 10 of the aforementioned Law foresees the general principles for that storage and the obligation that they be only the same data made available by judicial order.

424 The Civil Framework of the Internet is the result of a participatory process launched by the Legislative Affairs Secretariat of the Ministry of Justice, in association with the Center for Technology and Society of the Law School of the Getúlio Vargas Foundation in Rio de Janeiro, October 29, 2009. Based on the results of this first collaborative phase, the draft of the draft was formulated, which was again debated, in a second phase, in an open process that involved broad participation of society. The Internet Civil Framework was approved in the Federal Senate on April 23, 2014. See <https://pt.wikipedia.org/wiki/Marco_Civil_da_Internet>.

> "The custody and availability of the connection and access records to Internet applications covered by this Law, as well as personal data and the content of private communications, must guarantee the preservation of privacy, intimacy, honor and the image of the parties directly or indirectly involved.
>
> § 1 The provider responsible for the storage will only be obliged to make available the aforementioned records, autonomously or associated with personal data or other information that may contribute to the identification of the user or terminal, by judicial order, in the form of the provisions of Section IV of this Chapter, respecting the provisions of art. *7."*

In its article 13, the Framework states that in the provision of connection to the internet, it is a duty of the respective autonomous system administrator to keep the connection records under secrecy, in a controlled and secure environment, for a period of 1 (one) year, in accordance with the Regulation. And further, that only the interested party may for the purpose of forming a body of evidence in judicial, civil or criminal proceedings, incidental or autonomous, require the judge to order the person responsible for the storage the provision of connection records or access records to Internet applications, in accordance with the provisions of article 22 of this Law.

In art.15, the Internet Civil Framework refers to the application providers, defined as "the Internet application provider constituted in the form of a legal entity and that performs this activity in an organized, professional and economic purpose shall maintain the respective records of access to Internet applications, under secrecy, in a controlled and security environment, for a period of 6 (six) months, in accordance with the regulations."

It is noted then that the Internet Civil Framework brings two species of providers: connection and application providers . It also deals with data storage and its supply to the authorities. The issue becomes complex when these authorities need data from application providers (such as Facebook, for example) that are based outside of Brazil. Where are these data stored? Who should the authorities contact to obtain them?

Specifically, with regard to the production of criminal evidence, the Framework disciplines the way of obtaining data in its art.22:

> *'Art. 22. The interested party may, for the purpose of forming a body of evidence in civil or criminal proceedings, incidental or autonomous, require the judge to order the storage responsible for the provision of connection records or access records to applications of Internet.*
>
> *Single paragraph. Without prejudice to the other legal requirements, the request must contain, under penalty of inadmissibility:*
>
> *I - well-founded indications of the occurrence of the offense;*
>
> *II - reasoned justification of the usefulness of the records requested for the purpose of investigation or evidentiary instruction; and*
>
> *III - period to which the records refer.'*

Obtaining the records referred to in the aforementioned article 22, in cases where application providers store their data abroad, is not an easy task. For example, the controversy surrounding the obtention of the data of the WhatsApp application, which is dealt with in two actions in the Federal Supreme Court, is detailed below: the first, an Action of Non-compliance with a Constitutional Precept (ADPF 403), Reporting Judge Minister Edson Fachin and the second a Direct Action of Unconstitutionality (ADI 5527), from the Reporting Judge Minister Rosa Weber.

22.5 The Brazilian judicial battle in front of the WhatsApp application

On May 2, 2016, the Criminal Judge of the Lagarto Criminal Court, Sergipe, determined the suspension of the WhatsApp application service for 72 hours throughout the national territory. The determination was sent to the operators of Telefônica Vivo, Tim and Claro for the immediate fulfillment of that decision. This decision was due to the fact that Facebook, which acquired

WhatsApp, refused to provide necessary data for the criminal investigation.

The Popular Socialist Party, PPS, then brought before the Brazilian Supreme Court, STF, an accusation of breach of fundamental precept, with request for precautionary measure, "against the decision of the Judge of the Criminal Court of Lagarto (SE), Marcel Maia Montalvão, in the Process 201655000183, which blocked the WhatsApp communication application"[425]

The aforementioned argument – which brought ADPF403 MC before the STF – was based on the following arguments:

> *"The violation of the right to communication is crystal clear. In the end, the messaging application WhatsApp achieved something seen as unthinkable until the last decade: it united the most diverse generations in a single platform for the exchange of information, providing unrestricted communication for the adherents."*

And it proceeds to claim that:

> *"According to more recent data, of every 10 (ten) Brazilian cell phones, 8 (eight) are connected to the application. In a country of continental dimensions like ours, for a single mobile application to reach a number of consumers that reaches almost half of the Brazilian population, which is 205.8 million people, is something to behold."*

Finally, the author asserted that:

> *"The suspension of the activity of WhatsApp, based on controversial grounds, violates the right to communication, guaranteed constitutionally to the Brazilian people."*

Minister Ricardo Lewandowski, President of the STF, affirmed:

> "*Without going into the merit of using the application for illicit purposes, it is necessary to highlight the importance of this type of communication, even for the citation of judicial offices or decisions, as*

425 View <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403MC.pdf>.

> *reported by the electronic site <http://www.conjur.com.br/2016-27-Feb/Klaus-Koplinurgente-citación-hecha-WhatsApp>."*

As the Reporting Judge of the aforementioned ADPF 403, Minister Edson Fachin considering that the question deserved a technical analysis beyond the legal scope, called for a public hearing.

On the other hand, he also joined the STF with a Direct Action of Unconstitutionality brought by PR, the Party of the Republic, was distributed to Minister Rosa Weber (ADI 5527)[426]. It was decided then that the trial of ADPF 403 and ADI5527, which dealt with the same matter, were suspended for the realization of the aforementioned public hearing, and this hearing was finally held on two occasions: June 2nd and 5th, 2017.

It is known that judges can use technical evidence to support their decision. In this specific case, the public hearing convened by the Ministers of the STF also sought to obtain specific information on the matter under discussion in the actions in process, the criteria established for participation being: (i) technical representation,

(ii) Experience or expertise specifically in the matter and (iii) guarantee plurality of the composition of the audience and the points of view to be defended.

The representatives of the connection and application providers, the WhatsApp representative in Brazil and jurists were present at this public hearing, together with information technology experts, and representatives of connection and application providers. It is important to highlight the position of some of these experts who were present, in order to point out the complexity of the question of the production of evidences and the challenges faced by Brazilian authorities.

> "*-It is not up to us, nor to any sector, to discuss the investigative process. "We do not question the importance of cryptography, but we know that there are technical solutions that can be implemented by the provider to provide this information." Eduardo Levy informed that currently the Telecommunications*

426 View <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/AudinciapblicaADI5527.pdf>.

> *sector passes about 330 thousand information per year, without questioning any justice body. "The telecommunications sector attends to the legislation and, in our vision, WhatsApp must also do it (FEBRATEL: Brazilian Telecommunications Federation)".*

Information system specialist Volnys Bernal explained the technical aspects of logs, service blocking and interception of messages by telecommunication service providers, highlighting that "... cryptography is a reality and fundamental tool to ensure the security of communications and privacy on the Internet." He also indicated that the telecommunications service provider is capable of intercepting data traffic to meet legal demands.

> *"However, the data captured is rough. If it is encrypted, it is unfeasible computationally to decipher them, "he said. It was warned that the blocking of servers by the access and connection providers requires technical effort and that blocking is done from the list of network addresses provided by the applications. "However, it is not possible for telecommunication service providers to check if said information is correct and complete. For the fulfillment of the judicial mandates of immediate blocking of the service, that is a big problem. "That is because, he said, in those cases there is no working time for the discovery of the addresses of the servers or to measure the correctness of those addresses."*[427]

In the view of the lawyer Alexandre Atheniense, member of the Special Committee on the Law of Technology and Information of the Federal Council of the Brazilian Bar Association (OAB), "... Brazil cannot abdicate its legislation in favor of foreign companies." He criticized the reluctance of the international digital communication companies that act in Brazil to comply with what is determined by Brazilian legislation. He affirmed that it is inadmissible that those companies that have millions of users in Brazil use only their commercial interests to impose

427 See <https://cryptoid.com.br/banco-de-noticias/supremo-encerra-audiencia-publica-sobre-whatsapp-e-marco-civil-da-Internet/>.

their standards of conduct on the Brazilian market. The lawyer questioned why we should abdicate the application of Brazilian law in favor of a company that can leave Brazil tomorrow and leave everything behind, even referring to legal disputes[428].

In the case of WhatsApp, as the company says, it is not in a position to provide the data because they are encrypted and in this way, not even the company would have access to this data.

This is certainly a controversy that will still remain, from our point of view, without a short-term solution, as it constitutes a true "secret of the industry" of the company that manages WhatsApp, since it is related to key issues such as the technology used to develop the application and how to break it, which would mean, from the business point of view and its terms of use, a possibility of violation of the user's privacy and would impact the supply of its services throughout the world.

The fact is that WhatsApp, bought by Facebook, has its headquarters in a place ignored by the Brazilian authorities. And as cited in the decision that granted the precautionary measure ADPF 403, the application in question "... is used by 8 out of 10 Brazilians, in all areas: personal, commercial, and professional." It has already become absolutely indispensable to the life of Brazilians, but it also serves criminals, who migrated to the application. Not only because of the ease of use, but also because it is a difficult to monitor by the authorities, which determined the entire controversy involving the actions currently under way in the STF and cited above.

After the public hearing, the final judgment of ADPF 403 and ADI5527 is expected for the beginning of 2018. But if companies like Facebook and WhatsApp offer services in Brazil shouldn't they be subject to Brazilian law, or provide the data required by the authorities without restriction, in compliance with such legislation?

Regarding the issue, the Brazilian Public Ministry and the National Council of Attorneys General issued a technical note in 2016, in the sense that it is necessary "to alert Brazilian society

428 *Ibid.*

to the damage that is occurring to the investigations related to the various crimes practiced through the Internet due to non-compliance with Brazilian legislation by foreign companies that provide services in Brazil"[429].

The Technical Note states among other topics that:

> *"...On the other hand, article 11 of the MCI determines that the companies that offer services in Brazil (to Brazilians), despite not having subsidiaries here, must observe the Brazilian law regarding the collection, storage and processing procedures of logs, personal data or communications".*

The Note further states:

> **Sanctions**
> *Article 12 of the MCI seeks to ensure the effectiveness of Brazilian judicial decisions on the subject of Internet data. The main argument of companies for the non-provision of data transiting in online messaging applications or in social networks is that such companies are not subject to the Brazilian jurisdiction because they do not have headquarters in the country. The temporary suspension of collection, custody and treatment of personal data records, provided for in subsection III of Article 12, is a subsidiary measure to be adopted when other sanctions capable of inhibiting the breach of court orders, such as warnings, fines and blocking of bank accounts of these companies, are not enough to enforce current legislation. Such measures will be used whenever necessary, after the exhaustion of other less burdensome ones.*
>
> **Need for collaboration**
> *To enforce its institutional mission provided for in the 1988 Constitution, the Public Ministry has insisted on negotiating with Internet companies. However, up to now, progress has been absolutely unsatisfactory.*

429 View <http://www.mpf.mp.br/pgr/noticias-pgr/mps-alertam-para-descumprimento-da-legislacao-brasileira-que-regulamenta-uso-da-internet>.

Unlike what they claim, Internet application companies, such as Facebook and WhatsApp, do not fully and effectively collaborate, as required by Brazilian laws, nor did they express a real willingness to negotiate effective ways to provide immediate data determined by court order. Once these companies refuse to comply with Brazilian standards, the inadequacy of the service provided by them in the country is configured.

Internet crimes

The universalization of the Internet and the growth of human coexistence in the virtual world have exponentially increased the practice of cybercrimes and common but serious crimes, such as drug trafficking (domestic and international), dissemination of child pornography, racism, crimes of hate, patrimonial crimes and, at the moment in which the Olympic Games of Rio de Janeiro will begin, the crime of terrorism. The cooperation of the connection and application providers together with the Public Prosecutor's Office and with the Police is essential to stop or prevent these criminal activities"[430]

22.6 Conclusion

Digital inclusion in Brazil is increasing rapidly. However, in terms of criminal prosecution of cybercriminals, the current stage is of profound perplexity with the total impotence of the Brazilian authorities to obtain evidence for the resolution of crimes that increasingly migrate to the virtual universe. Today it is not necessary to make noise to rob a bank: a computer with Internet access is enough. It is a silent crime that produces immense damage.

Being prepared to investigate and punish these criminals is an urgent matter. In this country, in which violent crimes exploded again, virtual crimes are relegated to the background by the legislator, until something of repercussion occurs. For example, the Internet Civil Framework was only approved after Edward Snowden disclosed the espionage of then President Dilma Rousseff by the US government information agency NSA. The uncommendable

430 *Ibid.*

habit of "emergency legislation" has led to the approval of poor laws that do not meet the needs of the Justice System operators.

It is urgent that the discussion about the Budapest Convention be addressed in order to create effective mechanisms of international cooperation, updating existing mechanisms, such as the MLAT and investing in training of law enforcement agents, Judges and Prosecutors.

It would be ideal that these investigations were not necessary. The improvement in prevention activities and the dissemination of strategies focused on the general public, mainly children, must undoubtedly be the objective to be pursued.

22.7 References

Corrêa, G T (2000). Aspectos jurídicos da internet. São Paulo: Saraiva,. 135 p. p. 43.

Crozé, apud Ferreira I S (2001). A criminalidade informática, Direito e Internet – Aspectos jurídicos relevantes. Editora Edipro.

E Atheniense, A. (2010). "Apostila Curso de Direito e Tecnologia da Informação". ENA. Escola Superior da Advocacia.

Gomes, L F (2002). Atualidades criminais. Retirado de <http://www.direitocriminal.com.br>.

Greco, R. (2006). Curso de Direito Penal – Parte Especial. Ed.Impetus.

Inellas, G C Z de (2004). Crimes na internet. São Paulo: Juarez de Oliveira, p. 80.

Lima De La Luz, M. (1984). Delitos informáticos. México DF: Criminalia. Academina Mexicana de Ciencias penales.Ed. Porrua.

Paesani, L M (2006). Direito e Internet: liberdade de informação, privacidade e responsabilidade civil. 3 ed. São Paulo, Atlas, p. 26

Rossini, A E de S (2002). Brevíssimas considerações sobre delitos informáticos. Caderno Jurídico Direito e Internet. São Paulo: Imprensa Oficial do Estado. Escola Superior do Ministério Público.

Simoes, V F N (2012). "Legado Informacional dos órgãos públicos". Revista Fonte: PRODEMGE. Dezembro.

Simoes, V F N & Atheniense, A. (Março, 2010)"Apostila Curso de Direito e Tecnologia da Informação". ENA. Escola Superior da Advocacia.

23 Who is Responsible for Internet Security?

Carlos S. Álvarez

Note: this article reflects exclusively the opinion of the author and not, in any way, the opinions or official positions of the Internet Corporation for the Assignment of Names and Numbers, ICANN.

Abstract

Internet security is a matter for everyone. However, what does this really mean? When talking about *everybody* it is so easy to dilute personal responsibility until it almost disappears. The article provides elements of analysis in relation to the roles that correspond to the different actors and sectors in society and refers to the responsibilities that are expected to be honestly accepted and assumed voluntarily by each actor in society.

23.1 Introduction

Issues related to Internet security have been in vogue for several years. On these issues every day there are online articles, radio, television and press releases and, in general, about them. Users in general have become accustomed to receiving information very frequently.

However, this does not mean much. It suggests, of course, that the media remains interested in publishing related content because, obviously, it sells. The public is always interested in reading news about the latest attacks[431], about the latest companies that have been victims and the impact they have suffered, about the possible shame that the celebrity character who has recently been attacked is going through.

This reality would also suggest that users, both individual and corporate, of the education sector and government should be in the middle of a process of awareness that should lead gradually to increase their levels of security. That is to say, little by little they would be protecting in a more adequate way the information

431 See Newman (2017).

that rests in their information systems and the one they dispose physically and digitally, as well as information they send and receive, and network devices like servers, desktops, routers, switches and firewalls, in addition to all their portable devices.

But it also suggests that all the actors that can play some role in the joint task of making the Internet safer, would be aware of the importance of effectively fulfilling that role. For example:

- States may enact laws or regulations that require minimum safety standards for enterprises according to the sector to which they belong or, better yet, industrial associations may dictate their own self-regulation measures that create the expectation that each industry will do the voluntarily.
- Consumer protection associations can create and advance robust awareness campaigns within which information is given to users about measures that allow them to reduce their level of risk.
- Colleges and universities can include in their curriculums courses related to security from different perspectives, including aspects of awareness and basic prevention, technical aspects for those who want to know the technology in detail, business aspects for those who have a more managerial and strategic vision, in addition to the legal content related to security, technology and information that may be of interest to others.
- Internet service providers (ISPs) can voluntarily implement measures that have been defined by the technical community for several decades and which, because of the specific position they occupy, have a huge effect on reducing malicious Internet traffic (see BCP 38[432] and BCP 84[433] on source address validation and Open Resolver Scanning Project[434] on recursive and open DNS servers).
- Hosting service providers can secure their servers responsibly, reducing the number of compromises that are frequent victims who administer or operate websites.

---

432 See Ferguson & Senie (2000).

433 See Baker & Savola (2004).

434 The Open Resolver Scanning Project by Shadowserver can be found at <https://dnsscan.shadowserver.org/>.

- All entities in the financial sector can implement, at least, multi-factor authentication[435] to reduce the risk of the money from your clients' accounts being stolen when criminals manage to access their usernames and passwords.
- All entities in relevant sectors, such as the government sector, financial entities, security forces, owners of recognized brands and in general those who register domain names, can implement measures that prevent third parties from sending e-mail impersonating their domain (see Sender Policy Framework or SPF[436], Domain Keys Identified Mail or DKIM[437] and Domain-based Message Authentication, Reporting and Conformance or DMARC[438]).

Finally, without the desire to list here all the possible actors and all the roles that they can play, it is interesting to highlight how these mentioned examples highlight a fact that, although it is frequently repeated, probably has not penetrated enough in the public user of technology: Internet security is the responsibility of everyone, and everyone has to understand their societal roles and responsibilities.

23.2 Relationship between the model *multi-stakeholder* and Internet security

23.2.1 The *multi-stakeholder* model

When speaking of "all" one can have the feeling that this "all" is something ethereal, not concrete, that ultimately ends up dissolving the individual responsibility of each particular actor. This responsibility, however, has several natures, in some cases legal and in others ethical. Whatever the case, it is a responsibility that must be understood, assumed and accepted.

In the multi-stakeholder model, this responsibility of each individual actor is translated into effective action and active participation

435 See Alvarez (2017).

436 The Sender Policy Framework Project publishes information related to SPF in <http://www.openspf.org/>.

437 The dkim.org site publishes information related to DKIM in <http://dkim.org/>.

438 An explanation of how DMARC works can be found in <https://dmarc.org/ overview/>.

in the development of the discussions and policies on which the participating communities decide to work. It is a model in which all participants must speak the same voice and in which there is no actor that decides for others, or that prevents others from participating in decision-making.

Different versions of this model have been implemented in organizations related to Internet governance. The Internet Corporation for the Assignment of Names and Numbers (ICANN)[439], is perhaps the best example. Within ICANN, representatives of all communities contribute, from governments through its Governmental Advisory Committee (GAC)[440], to public safety agencies[441], going through defenders of individual freedoms and users in general[442], financial entities and large or small companies[443], holders of trademarks and copyrights[444], security experts[445], root server system operators[446], domain operators of high level[447], domain name registrars[448] and other interested parties. All of them can participate and influence the development of the policies related to the Domain Name System in particular, and, in general and to a certain extent, with the unique identifier systems of the Internet.

As for the Domain Name System, the multi-stakeholder model has produced tangible results as evidenced over the years with effective policies such as the Uniform Domain-Name Dispute Resolution Policy or UDRP[449], which has allowed so many owners of intellectual property rights to defend their brands in certain situations. Or the policies related to the renewal and expiration of

439 See <https://www.icann.org/>.

440 See <https://gac.icann.org/>.

441 See <https://gac.icann.org/working-group/gac-working-group-on-public-safety>.

442 See <https://atlarge.icann.org/>.

443 See <https://gnso.icann.org/en/commercial-and-business/>.

444 See <http://www.ipconstituency.org/>.

445 See <https://www.icann.org/groups/ssac>.

446 See <https://www.icann.org/groups/rssac>.

447 See <https://gnso.icann.org/en/about/stakeholders-constituencies/rysg>.

448 To see in <http://icannregistrars.org/>.

449 See <https://www.icann.org/resources/pages/help/dndr/udrp-en>.

the domain names (Expired Domain Deletion Policy or EDDP[450] and Expired Registration Recovery Policy or ERRP[451]), whose correct implementation prevents those who have registered domain names from losing them due to their non-renewal and allows for recovery under certain conditions.

This model can be used in any social, economic, legislative or political sphere and, since cybersecurity has diverse expressions in all these areas, it has also been used in processes related to Internet security and other related topics. The next section refers to the different roles that correspond to the multiple stakeholders in terms of, precisely, cybersecurity.

23.2.2 Parties interested in Internet security

Now, how can Internet security be approached from the perspective of the multi-stakeholder model? Maybe the best way to do it is from the bottom up, following the same approach that is the essence of the model. That is, going from least to greatest, from local to regional and from domestic to global. In other words, the very thing that is controlled by each user to what we all share.

23.2.2.1 The role of the personal user

Rather than being corporate, government or any other sector users, and much rather than representing companies, governments, universities, and security forces or any other kind of entity, we are all personal users. And, as such, there is no distinction in relation to the role we all play as individuals: without going to the irrational extreme of demanding or expecting from non-expert personal user's certain safe behaviors or the implementation of complex solutions, it does seem reasonable to expect them, in general, to take basic measures that allow them to protect their devices, their communications, their privacy and their private life, their information and, logically, their money in the bank.

The primary responsibility of a personal user is to protect their own information and that of their family members. Before the

450 See <https://www.icann.org/resources/pages/registars/accreditation/eddp-en>.

451 See <https://www.icann.org/resources/pages/errp-2013-02-28-en>.

personal user, diverse sectors of the society have responsibilities, like providing education in matters of security online on the part of colleges, universities and unions of retailers, or providing robust and safe technological infrastructures on the part of, for example, the ISPs, of the financial sector or of the State itself.

This personal role has a scope restricted to the intimate and to the interaction of this field with the sphere of the public. And, as is logical, if the different sectors of society do not fulfill their responsibilities, such as providing adequate education, the personal user will not be able to assume his role and his own responsibilities.

23.2.2.2 The role of the corporate user

In addition to being personal users, some have an additional role that places them as members of an entity or a community. Public officials, employees of companies in different sectors, providers of medical, legal, accounting or any other services.

This second role has a different scope of responsibility, consisting of avoiding putting at risk or harming the information of the employer or their business environment (customers, suppliers and occasional third parties). Approaching this second role delineates a difference compared to the first, regarding the personal user, although he has a responsibility to his information and that of his family, this is fundamentally ethical order, being of a legal nature usually only when it comes to protecting the privacy of others, such as the spouse or minors. That is, in general, the law does not mandate that each user must protect their privacy or even their own assets.

For its part, this second role, which can be called corporate, often has legal and contractual responsibilities against the employer. These responsibilities range from loyalty due to specificities that may reflect detailed compliance with security standards, logically passing through the intermediate point where responsibilities exist, even if they are general. In face of the corporate user, the employer has the responsibility to properly educate him on cybersecurity, so that he can assume his own role as user and its corresponding responsibilities.

This corporate role focuses on strengthening behaviors that reduce the level of risk in the business environment. In fulfillment of this role, the user must, for example, be very attentive to attacks from *phishing* directed or *spear phishing*[452], which are a preferred route for attackers to gain access to the networks of their victims. One should be very cautious in relation to the content they access via the web or simply through the use of corporate devices or through a corporate network, as an attack by malware can end the reputation of a company, generate the obligation to pay huge sums as compensation to those affected, generate legal responsibilities of different orders if they are entities supervised by control agencies in their own jurisdiction.

23.2.2.3 The role of technology product and service developers

A third role is played by those who develop or sell technology products or services. Their responsibility is not only that their products and services fulfill the function for which they were created, but extends to seek to be safe and to not be easily abused by criminals to victimize their users or, worse, as platforms to attack against third parties.

The responsibilities that correspond to this third role are usually, primarily, of a contractual nature when they derive from agreements between developers or producers and their customers, or relating to regulations on consumer protection or even unfair competition.

It is worth mentioning the producers and distributors of products that can be considered as *Internet things*, that is, connected devices that are part of the *Internet of Things*. Their responsibility would be to make those *Internet things* safe, a feature that is still usually absent in this class of devices.

23.2.2.4 The role of infrastructure operators

A fourth role is one corresponding to those who operate network infrastructure, both internal and public Internet as such, or infrastructure associated with online services. Similar to the

452 The Federal Trade Commission offers information about what phishing is <https://www.consumer.ftc.gov/articles/0003-phishing>.

role of those who develop or produce services or products, the role of infrastructure operators is not only to provide the service to their clients, but to ensure that the service provided is not abused by criminals.

Infrastructure operators have a greater responsibility than those who play other roles, since what they do, frequently, is to provide bandwidth for the operation of their clients' businesses, which makes them an obvious objective for a lot of attackers looking for ways to multiply the bandwidth they have to increase the impact of their attacks.

23.2.2.5 The role of academic researchers

A fifth role is played by those who work in research and development. Depending on the object of the research, if it is looking for the development or improvement of new technologies, researchers should look for these new technologies to be safe and not become another vector of attack available to criminals. If, on the other hand, the object of the research is the development of technology focused on the provision of security on the Internet, they should seek that the technology in itself is not vulnerable and can be compromised by attackers who seek, for example, to manipulate it to avoid detecting a certain class of attacks or to manipulate the results of an investigation.

They should also seek to ensure that the implementation of the technology complies with the applicable regulations in each jurisdiction, in relation to the types of information that will be investigated and from which data are stored, as well as in relation to the obligations related to the chain of custody and compliance with the processes that guarantee respect for the law, both in relation to the satisfaction of information requirements by law enforcement agencies, and in relation to the privacy of personal information that may be stored or processed .

23.2.2.6 The role of law enforcement

The last two roles correspond to branches of the State. The sixth, then, is the fulfillment of the law from the perspective of the police agencies and the investigative entities of the State that should not

only protect their infrastructure and their investigations against the attacks of many possible adversaries, but also seek to be more efficient in the detection, mitigation and containment of attacks that affect citizens and organizations in their jurisdictions. This first aspect of this role of the branches of the State is similar to the role of those who operate network infrastructure and the responsibilities that correspond to it.

In addition, police agencies and state investigative agencies have the duty to identify, capture and prosecute those responsible for online criminal activity. This second aspect logically implies that state authorities should be able to pursue all forms of criminal activity online, logically respecting due process.

They must also have sufficient resources to fulfill their role, in terms of the knowledge required to identify the criminal activity as such and who is responsible for it, such as in relation to resources of appropriate technology and availability of sufficiently trained personnel.

23.2.2.7 The role of the legislator

The second role that corresponds to the branches of the State is the creation of the laws and regulations that are necessary in each jurisdiction on issues related, among others, with the definition of minimum levels of security for certain sectors, the definition of activities considered as harmful and their punishment, the implementation of state policies related to Internet security, and the standardization of substantial criminal and procedural laws at the international level. Logically, the responsibility of the State in this role consists of being proactive, efficient and effective in identifying areas that require new regulation, or whose regulation must be updated, as well as in the identification of areas that should not be regulated.

In addition, this responsibility also implies that the State must be open to listen to users and all sectors, and advance its regulatory and legislative processes in order to take into account their participation and identify the most efficient and sustainable solutions to achieve the objectives: protecting the rights of the ciitzens.

There are some additional responsibilities that, depending on the system of government of the countries, may correspond to a greater or lesser degree to the Legislative or the Executive, headed by the president:

- Identify and prioritize the resources available to face online threats (usually, this is part of the national security strategy of the countries, so in strict sense corresponds to the Executive. However, there are regimes in which budget appropriation is approved, or even defined, by the legislature).
- Define the relevant terminology regarding cybersecurity (with the ever-present risk of non-standardized definitions that further distance national legislations).
- Define general principles and specific provisions, such as legal assets to be protected and penal types to be sanctioned, related to online criminal activity.
- Define general principles and specific provisions on international cooperation, even though it is usually the Executive who is responsible for defining and directing the international policies of the states.

23.2.2.8 The role of incident response teams

There is an atypical role that can be assumed by corporate users, infrastructure operators, and by those who are linked to research and development or are officials of branches of the State, which consists of the provision of incident response services. Because the response to incidents is a necessity at all levels and this service is offered in a specialized manner, rather than a role, it is a function that can, and perhaps should, be performed in each sector.

There are response teams of very different natures, with very particular approaches. Some focus on protecting the online infrastructure of government sector entities, while others concentrate on protecting the infrastructure of the entity that created them (a university, for example). Others, independently, offer commercial services of protection and investigation of threats to organizations, while others can concentrate only on the implementation of security patches, for example.

And within this variety of activities that the response teams can provide, they can have different approaches: from the implementation of security standards, to the investigation and proactive detection of threats and infrastructure used in attacks[453]

23.3 A comprehensive approach to security

23.3.1 Inter-dependence relations

Security cannot be seen from the perspective of isolated silos. That is to say, among all the roles that revolve around security on the Internet there are strong relationships of interdependence. It is not possible to think of a generalized acceptable level of security if each one does not honestly assume the responsibilities proper to the roles that correspond to him. For example:

- If the colleges and universities do not comply with the personal user with their responsibility to provide education oriented to issues related to online security, that end user probably does not have enough elements to adequately assume his role as a personal user to protect properly. Your personal information and that of your family, and corporate information regarding your employer and business environment, will be subject to unnecessary online risks.
- If the developers of technology products and services do not adequately insure them, those products and the provision of those services will assuredly become vectors of attack exploited by criminals in the commission of their illegal activities. An example of this situation is the attack directed against Dyn in October 2016[454], which resulted in the temporary decline or serious degradation of Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix services, in which, at least partially, the Mirai botnet recruited thousands of devices from the Internet of Things[455], particularly video cameras and digital recorders, to be used as vectors in the attack. The recruitment of all these devices

453 You can consult about information related to response teams to indicentes on the Forum of Incident Response and Security Teams website or FIRST, in <https://first.org/>.

454 See York (2016).

455 See Krebs (2016).

was made possible because their factory configuration was particularly flawed and allowed attackers to take remote control of them very easily.

- If corporate users are not responsible for their behavior on your company's internal network and in relation to your customers and suppliers, they can easily be the point of entry for any form of malware or the weak point through which information is leaked[456]. And clumsiness, laziness, negligence or simple lack of diligence can easily lead to a corporate user clicking on a link that leads to downloading malicious code or revealing information to an adversary. Or you can have that user forward, without knowing that it is being used for the purpose by an attacker, a malicious attachment to a colleague in order to compromise your device and, from it, the entire network.
- If governments and legislators, each in their area of competence, do not produce or update the regulations that are necessary to keep the legal system up to date, as technology advances in relation to online security, it will be more difficult for those who are affected by the contractual or quasi-contractual negligence of third parties seek civil compensation for their damages, or it will be more difficult for insurance companies to issue policies that transfer the *cyber* risk *that face their clients*, or it will be simply impossible to pursue certain harmful behaviors through criminal proceedings due to their non-typing.
- If hosting service operators do not properly secure their servers and their clients' websites are compromised, they can be used both to distribute malware, as command instances, and to control infrastructures that direct attacks through ISPs that do not filter source IP addresses and who's DNS servers are configured openly, without any implementation of rate-limiting[457]. And the victims of these attacks will not only be those targeted by malicious traffic, there will be many users who will be affected by the depletion of the resources of the infrastructure operators that are impacted by the data overload. These include emergency response services such as ambulance, police and rescue, tele-medicine services,

456 See McCandless (2018).

457 See <https://en.wikipedia.org/wiki/Rate_limiting>.

ground or air traffic control, critical infrastructure facilities such as hydroelectric power plants, telephony and control of energy services in geographical areas, among many others.

These simple examples serve as a reminder of the relationships that exist between different roles in society. Not accepting the responsibilities that correspond to each role generates consequences that may affect whole sectors, geographic regions, population groups, user classes or groups of companies.

23.3.2 A successful example: The Mexican National Cyber Security Strategy

The Cybersecurity Program of the Organization of American States (OAS)[458] this year convened a technical mission whose objective was to facilitate the creation of the National Cyber Security Strategy in Mexico[459]. This effort is worth mentioning as it had the participation of all sectors of Mexican society, in a process that was facilitated by a group of international experts, in which the author of this chapter had the honor of participating under the leadership of the OAS.

State security agents, academics, representatives of the private sector, prosecutors and representatives of the public prosecutor, defenders of individual liberties, users in general, all had the opportunity to participate in various ways in the process that ended with the publication of the Strategy National. The discussions revolved around the legal framework, the educational system and the Mexican cultural reality, academic research, cooperation and international coordination and between the private and public sectors, technical standards and regulation and critical infrastructure.

And, in a real and tangible way, the Mexican government listened to all sectors and took into account its vision, from issues of pure security to those related to human rights.

More interestingly, all sectors wanted to participate in the development of the National Strategy that would affect them once

458 See <https://www.sites.oas.org/cyber/Es/Paginas/default.aspx>.

459 See <https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad>.

it was enacted. And, in a consistent and responsible manner, they effectively got involved and expressed their points of view.

It is worth mentioning here a relevant part of the document, which clearly shows how the multi-stakeholder model was chosen by the Mexican government and the OAS for the development of the Strategy:

> "*The National Cybersecurity Strategy defines objectives and cross-cutting axes, captures the guiding principles, identifies the different actors involved and provides clarity on the articulation of efforts between individuals, civil society, private and public organizations in the field of cybersecurity; It also points out the governance model for the implementation, monitoring and evaluation of the Strategy.*
>
> "*In Mexico, the Government of the Republic, in its role as facilitator, promoted spaces for dialogue, discussion and learning through forums and workshops in a collaborative process called "Towards a National Cybersecurity Strategy" from March to October 2017. In these spaces, the different actors of the society shared ideas, concerns and proposals on cybersecurity that showed great coincidences on the needs that the Strategy should address, such as:*
>
> - *"That the ENCS articulate the development of cybersecurity actions that serve individuals, companies and public institutions of the Mexican State.*
> - *"Collaboration and cooperation among the different sectors as a key element for the development, monitoring and evaluation of the Strategy.*
> - *"Know the dimension of risks and threats in cyberspace, the state that keeps cybersecurity in the country, the construction of a national diagnosis, as well as obtain evidence to improve decision making in cybersecurity.*

- *"Contemplate the global scenario as part of the problem and diplomacy as a way to establish dialogues and agreements that allow facing risks, threats and cybercrimes.*
- *"Develop specialized human capital in the field of cybersecurity.*
- *"Promote the responsible use of ICTs and reinforce a culture of cybersecurity that includes awareness, education and training actions".* (The underlining is ours)

The articulation of all sectors of Mexican society and their effective linkage to the process facilitated by the government and the OAS deserves recognition. Each sector identified the role it should play, assumed it and acted consistently. Similar processes have been experienced in other countries of the region, although these are the large minority to which the initial part of the next section makes brief reference.

23.4 Responsibilities of the states and the ISPs

This section will refer in a timely manner to the responsibilities that correspond to the states and Internet infrastructure providers, according to their specific roles. They, as far as each one is concerned, have a particularly important role in maintaining Internet security in favor of all users, the private sector, public entities and other actors in the international context.

Precisely because of the importance of their role they should serve as models for other sectors of society. They are at the forefront of these other sectors in terms of access and security on the Internet and it is expected that they lead by example, encouraging society as a whole to assume the role that each one corresponds with namely responsibility and mature conscience.

This brief analysis about the states and the ISPs then will help us to suggest an answer to the question of whether they have assumed reasonable responsibilities and if they are acting in accordance. Or if, on the contrary, both continue in unconsciousness towards the role that they should actually assume.

23.4.1 Responsibilities of States.

In the definition of its Strategy, Mexico joined the group of countries made up of Colombia, Jamaica, Panama, Trinidad and Tobago, Uruguay, Brazil and Costa Rica, which have already defined theirs. And, even though the fact that these countries have taken this step is very positive, on the other hand, the vast majority of countries in Latin America and the Caribbean have not yet done so.

Added to this is the current status of accession and ratification to the Budapest Convention by the countries of the region, of which only four have acceded to the convention and ratified it[460]. The regional situation is complex because countries generally have insufficient legislation, although they can deal with issues related to privacy and data protection, or can even define some criminal types and include criminal procedural rules that attempt to address related processes. With cross-border digital investigations, information sharing and digital chain of custody, in general the legislative and regulatory backwardness in the region in terms of cyber is such that there is no standardization neither in substance nor procedurally, so the criminal system, which acts as a final sanction, simply does not reach the cybercriminals in a continuous and efficient manner.

It is also worth referring to the weaknesses of the judicial system of the countries in the region, in which investigators, prosecutors and judges often do not have sufficient technical knowledge to understand the conducts they must investigate or judge, and do not have infrastructure, tools, equipment and necessary processes for the work. In the latest report on the state of the region (Cybersecurity: Are we ready in Latin America and the Caribbean?[461]), prepared by the Organization of American States and the Inter-American Development Bank, Hathaway, McArdle and Spidalieri, all from the Potomac Institute, clearly indicated

460 The text of the Budapest Convention is available in <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>. The situation regarding the Budapest Convention in the region is frustrating for some, including the author of this chapter who, almost 15 years ago, published his first notes and gave his first talks related to this topic and about the importance of countries join the Convention. At that time, he even had the opportunity to ask directly to Colombian President Álvaro Uribe, who basically had no information about it and whose government focused on the free trade agreement with the United States, leaving aside, unnecessarily, the Budapest.

461 See Inter-American Development Bank (IDB) & Organization of American States (OAS) (2016).

that "*Most countries have insufficient forensics capabilities to investigate and prosecute crimes, or the criminal justice system has not developed the capacity to handle electronic evidence or enforce existing and updated cybercrime laws*"[462]

The great majority of States in our region are still unclear about the role and responsibilities that correspond to each one in relation to Internet security or, if they already have that clarity, they have not yet decided to assume that role and comply with what it demands. And this is a debt that is paid every day in terms of the damage caused by online attacks against public entities, the private sector and end users. Sooner or later the bill will reach the states, or at least it is reasonable to expect this to happen.

The states' responsibilities in terms of cybersecurity cover issues such as the development of strategies and programs to increase the sharing of information on threats between the private sector and security agencies, the definition of the national cybersecurity strategy of each country, the creation and implementation of education programs for different sectors of society and the search for appropriate legislation in criminal matters (both in terms of substantive law and procedural law), in civil matters (foreseeing, for example, civil causes that can be initiate for the repair of damages caused by harmful conducts through the Internet), among others.

23.4.2 The responsibilities of those who provide Internet infrastructure

The providers of Internet access services, or ISPs as they are usually known, have a particularly important place in the fight against forms of criminal or malicious activity on the Internet. They are both a first line of defense that can prevent malicious traffic from leaving devices controlled by criminals to the public Internet, and a last line of defense that can prevent malicious traffic from reaching the end users from the public Internet.

ISPs usually not only provide the connection service, that is, they

462 "Most countries have insufficient forensic capabilities to investigate and bring criminal cases before judges, or the judicial system has not developed the ability to administer electronic evidence or enforce existing or updated laws."

usually offer other services as well. And one of these services consists of having DNS servers that resolve the domain names for the devices of their clients. What does this mean? That, in general, the ISP from which users receive their Internet connection has provided a server that will help them find the IP address where the server that hosts the content of the news site they want to visit is located.

And the way in which these resolution servers are administered clearly indicates if each ISP in particular has recognized its role, in terms of Internet security in front of the general public and in front of its own clients, or not. Many ISPs manage these servers in a poor way, answering unlimited queries about domain names sent by users located in any country, even if they are not their own clients. And, when these servers are managed in this way, they are used as a vector in large distributed denial of service attacks[463]. These servers are known as open resolvers.

According to the information provided by The Shadowserver Foundation through its DNSSScan[464], as of December 14, 2017, date of consultation of this information, 18,111 open solvers were detected in the Caribbean region, 41,789 in Central America and 271,996 in South America. According to the observations and analyzes of Shadowserver, the five countries in which there are more open solvers in the region are Brazil (166,108), Ecuador (31,613), Argentina (29,906), Mexico (26,496) and Colombia (16.103)[465].

On the other hand, the five countries with the highest proportions of open solvers according to the size of their IPv4 space (according to the data published by RIPE NCC that come from LACNIC[466]) are Belize (3.16%), Ecuador (1.21%), Guyana (1.11%), Bolivia (0.66%) and

---

463 See Alert TA13-088A from the US-CERT about amplification attacks via DNS, available in <https://www.us-cert.gov/ncas/alerts/TA13-088A>.

464 The Open Resolver Scanning Project by Shadowserver is available in <https://dnsscan.shadowserver.org/>.

465 Crossing this information with available data About the IPv4 space in the region, four of these five countries are in the group of the five with the most IPv4 space, except for Ecuador, which would be in the ninth place by size of its IPv4 space.

466 RIPE NCC publishes statistics provided by LACNIC through <ftp://ftp.ripe.net/pub/stats/lacnic/>.

Dominican Republic (0.58%)[467]. And, additionally, the countries in which there is a greater number of solvers opened by ASN (that is, for each range of IP addresses that has been assigned or delegated by LACNIC in each country) are Belize (116.71), Ecuador (102.97), Dominican Republic (85.94), Uruguay (75.30) and Bolivia (75.05).

Initially, the logical conclusion is that ISPs have not, in general, accepted their responsibility in maintaining a clean Internet, with less malicious traffic. However, it is necessary to see between the lines when analyzing these data that have just been offered, since these numbers are surely related to the number of compromised devices within each IP address range (within each ASN), which would mean that it is possible that not all the open resolvers identified by Shadowserver are being managed by the ISPs directly. Rather some of them are compromised devices that are resolving names due to the commitment to malware to which they were subjected (for example, in Ecuador there are 305 IP address ranges delegated by LACNIC but Shadowserver identified more than 30,000 open solvers).

However, even if this is the case, that is, even if the ISPs are not directly managing all the open resolvers that were identified, these numbers continue to indicate that ISPs have definitely not accepted their responsibility in maintaining Internet security. The inevitable suspicion arises that they are not filtering the IP addresses of origin and are answering queries sent by any user, including devices that are part of botnets, falsifying the IP address they claim to come from so that the resolvers become cannons that shoot huge amounts of data against the victims.

It is worth mentioning that the technical community published the first IETF draft[468] on the subject in 1997, which then became RFC 2267[469], and that was finally replaced by RFC 2827[470] to end

467 This proportion is obtained by dividing the total of open solvers identified by Shadowserver by country, by the total space in IPv4 of each country according to the information published in the link included in the footnote above.

468 The Internet Engineering Task Force explains what an Internet Draft is <https://www.ietf.org/id-info/>.

469 Ferguson & Senie (1998).

470 Ferguson & Senie (2000).

up becoming the BCP 38[471], which is complemented with the BCP 84[472]. That is to say, almost 21 years ago the technical community defined an accepted and standardized form that the ISPs can voluntarily implement to avoid the traffic that falsifies the IP addresses of origin to pass through its routers. And yet the ISPs still do not implement these technical measures.

23.5 Conclusions

Clearly, neither the states nor the ISPs have assumed the responsibility that corresponds to them when it comes to making the Internet safer for all. For reasons that are apparent, the states still do not see the reality in which we have been immersed for several years and the ISPs are still focused on seeking to make their businesses more profitable (which is legitimate) but they forget their social responsibility related to reducing the malicious traffic that abuses its networks and that affects the generality of users on the Internet.

It is appropriate to compare the region of Latin America and the Spanish-speaking Caribbean (the region that corresponds to LACNIC) compared to the other regions according to each corresponds to a regional registry of different Internet. According to the analysis of Team Cymru[473], the LACNIC region presents malicious activity from 32% of the IP addresses advertised in it, while for the region of Europe and the Middle East (RIPE NCC) this percentage is 29%, for Asia Pacific (APNIC) it is 80 %, for Africa (AfriNIC) is 3% and for North America and the English-speaking Caribbean it is 5%.

Our region is not in the worst 80% scenario but it is far from 5% in North America. There is a long way to go. That a third of the IP addresses advertised in the region are being used by criminals to send malicious traffic, according to the observations of Team Cymru, should be simply alarming.

---

471 *Ibid.*

472 Baker & Savola (2004).

473 Team Cymru publishes its Hackbook, which presents statistics by country and region on topics such as assignment and announcement of IPv4 and IPv6 space, as well as malicious activity, in <https://hackbook.team-cymru.org/>.

And the percentage is so high because in all sectors of society, logically including personal users, corporate users, those who operate Internet infrastructure, those who develop or market products or services online, in short, all, lack of awareness of the role that corresponds to each one. And this lack of awareness leads logically to ignore the responsibilities to society that are specific to the place where each one is.

So, answering the question posed in the title of this article, who is responsible for Internet security? It is not possible to arrive at a different answer than "everyone". All actors and all sectors of society that have access to technology resources have a role to play to which particular responsibilities correspond.

Without pursuing the utopian scenario in which those responsibilities are honestly assumed by all, this writing provides some elements of analysis seeking to enrich the discussion from a social perspective. It can also serve as a support point for the implementation of programs or activities that facilitate the participation of all parties in the search for that safer Internet to which we are all entitled.

Be a corollary that serves as a principle to guide the path we all follow as a society, individually and in partnership with others, towards that better and safer Internet:

> *I acknowledge and accept the roles that correspond to me regarding Internet security and I assume the responsibilities of each role.*

23.6 References

Alvarez, M. (2017). Is Multi Factor Authentication The Best Cyber Security Method? Forbes. <https://www.forbes.com/sites/quora/2017/12/04/is-multi-factor-authentication-the-best-cyber-security-method/#21ac89e07c4e>.

Baker, F. & Savola, P. (2004). Ingress Filtering for Multihomed Networks. Internet Engineering Task Force. <https://tools.ietf.org/html/bcp84>.

Banco Interamericano de Desarrollo (IDB) & Organización de los Estados Americanos (OEA) (2016). Cybersecurity: Are We Ready in Latin America and the Caribbean? IDB. <https://publications.iadb.org/handle/11319/7449>.

Evans, M. & otros (información actualizada a febrero de 2018). World's Biggest Data Breaches. Information is Beautiful. <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>.

Ferguson, P. & Senie, D. (2000). Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. Internet Engineering Task Force. <https://tools.ietf.org/html/bcp38>.

Ferguson, P. & Senie, D. (1998). Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing – RFC 2267. IETF. <https://www.ietf.org/rfc/rfc2267.txt>.

Ferguson, P. & Senie, D. (2000). Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing – RFC 2827. IETF. <https://www.ietf.org/rfc/rfc2827.txt>.

Krebs, B. (2016). Hacked Cameras, DVRs Powered Today's Massive Internet Outage. KrebsonSecurity. <https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/>.

Newman, L. H. (2017, 7 enero). The Biggest Cybersecurity Disasters of 2017 So Far. Wired. <https://www.wired.com/story/2017-biggest-hacks-so-far/>.

York, K. (2016). Dyn's Statement on the 10/21/2016 DNS DDoS Attack. Dyn Blog. <https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/>.

24 The Legal Framework for Cybercrime

Horacio Azzolin

Abstract

The emergence of the first cyber-crimes allowed us to realize that most Latin American countries were not sufficiently prepared to face this phenomenon. Over time, we have learned that researching these cases requires the states to be prepared in many ways. The adoption of a national cyber security strategy, the establishment of cyber incident response centers, the support of prevention campaigns for citizens and keeping properly equipped and trained police forces are some examples. An issue that, for various reasons, is sometimes left out is the regulatory system. In some way, fundamental laws which define crimes establish the rules of procedure, and mechanisms for international cooperation are also needed. Sometimes, they are even indispensable. The article proposes the revision of the most important aspects that police and manufacturers should take into account when reviewing the legislative system of their countries.

24.1 Introduction

I want to introduce ourselves to this topic without delay. The Internet is constantly growing, more and more users are doing more and more things with it. Criminal organizations noticed this phenomenon and mutated part of their activities in the Internet, using it as a tool to commit known crimes. We called them *computer related crimes,* or just *computer crimes*.

The emergence of the first crimes committed through or against computer systems allowed us to realize that our countries were not sufficiently prepared to effectively process these cases. Although at present the situation may have changed in some aspects, there is still a long way to go. A good part of that road is related with norms. My proposal is that we review the issues that must necessarily be touched in order to establish an adequate legal framework to face this phenomenon.

As I anticipated, the legal system of most countries in Latin America was not prepared to face cybercrimes for the simple reason that they did not exist when the laws were established. The lack of preparation was often taken into the basic concepts of the penal codes, which define that human actions like killing someone for example, constitutes a crime, laws did not foresee these new criminal modalities whose means and objectives may be immaterial.

For this reason some years ago there was an idea, for example, to frame a criminal case of fraud when the victim was not a person but a computer system, in cases of fraud using ATMs, for example, or if the damage could also fall on immaterial things, such as data.

Although most countries have made progress in this regard, approving reforms to their penal codes during the first years of the 21st century, new criminal modalities have emerged since then. The unauthorized dissemination of intimate images, the take over of another's identity, the capture of personal data under deception, the increasingly massive attacks of denial of service, among others, are some of the new threats that deserve the attention of the *policy makers* in general and legislators in particular.

The criminal procedure laws (which establish how the trials are conducted and, fundamentally for this article, how the evidence is collected and valued) were also not prepared since they only had provisions to obtain and process physical evidence. Then, the seizure of the data contained in a storage device, for example, was not considered in the law. The law only allowed the seizure of the physical container of that data, that is to say the computer, the notebook or another device in which the hard disk were kept and installed.

24.2 An adaptation to the digital environment

The normative deficiencies were increased to the extent that computer systems took a more prominent role in our lives. In the first place, in the recent past our images, our messages, our contact list, our to-do list and our sensitive information were stored in our households in independent physical media. In this way, a researcher looking for a photo, only had to review an album without the need, for example, to review our contact list, or our mail.

All this information is now stored in digital format and instead of being in our households we carry it on a phone, a tablet or a laptop. From a practical point of view, this means that searching for that same photograph today may involve reviewing other information and, therefore, it implies the invasion of our privacy in a much stronger way than before. This is why today the tendency in the courts in relation with procedural guarantees is to grant greater protection to the digital environment than to the domicile itself[474].

On the other hand, the irruption of Internet has generated changes in our habits. Among them, our way of communicating (from phone and mail to voice calls over IP, text messages and instant messaging and emails), the way we search for information (Internet search engines and social networks have replaced libraries and newspaper) and the way we get entertained (we access more content by *streaming* than in the cinema or the television). Researchers have investigation techniques which are not designed for those new environments. For example, laws authorize to follow a suspect when going to a library to see what books are consulted by the suspect, or what things someone looks for in the supermarket, but it does not allow the same activities if someone searches for the same things through the Internet. The possibility to remotely access computer devices to monitor a suspect's online activity – provided due process respecting the individual and the principles of the rule of law – is something that procedural laws must address. This, in turn, will generate new debates about the type of tools that will be used, who will design them, how it will be installed and how it will be audited, and in what way it can serve as evidence in a trial.

As explained before, information was originally stored in physical containers (photo albums, accounting books, etc.) and they started to be stored in digital format through notebooks and other connected devices. This also has experienced some changes, since now it is possible to storage information in third-party devices, which may or may not be located in the same country where the owner of the data lives.

474 See, for example, the judgment of the European Court of Human Rights "Trabajo Rueda c. Spain "of May 30, 2017 where the procedure for seizing data in a computer was questioned, considering that the right to privacy of its owner had been violated.

The possibility of hosting and storing data in other jurisdictions thanks to the services of "cloud storage"[475] also generates jurisdiction problems: data is accessed from country A, but physically stored in country B (or part in country B and part in C, as it happens more and more often). From a traditional conception of the regulation of proof, the judge of country A could only access the information stored in B (or B and C) through a request for legal assistance, usually regulated by the so-called *Mutual Legal Assistance Treaties (MLAT).* This process takes a long time and can affect the success of the investigation, because while the request is processed, there is no control of the data that can be eliminated remotely. We must also rethink, then, the rules of obtaining proof abroad, abandoning criteria of territorial sovereignty which is incompatible with the dynamics of the internet.

And speaking about international cooperation, it is closely linked to cybercrime investigation. And the reason is simple: international crimes require international investigations; and international investigations require international cooperation. In most cases in which we have intervened, there was an international factor: part or the whole evidence of the case information was stored in servers located in another country[476], sometimes the accused or the victims were also living abroad. So, it is necessary that all nations agree on the way in which they will cooperate with each other to investigate this type of behavior.

24.3 The Budapest Convention

Taking into account the scenario described, the Council of Europe sanctioned, in the year 2001, the Convention on Cybercrime[477] (also known as the Budapest convention or convention, for its place

475 The term storage in the cloud, from English *cloud storage*, refers to "a data storage model based on computer networks, where the data is housed in virtualized storage spaces, usually provided by third parties. Hosting companies operate huge data processing centers. The users that require these services buy, rent or contract the necessary storage capacity". See <https://es.wikipedia.org/wiki/Almacenamiento_en_nube>.

476 To demonstrate that, we can see how requests for information to Google Inc. from Argentina went from 98 in the second half of 2009 to 491 in the first half of 2017 <https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts;authority:AR&lu=user_requests_report_period>. In the case of Facebook Inc., orders went from 152 in the first half of 2013 to 984 in the first half of 2017 <https://transparency.facebook.com/government/about/>.

477 See <http://www.oas.org/juridico/english/cyb_pry_convenio.pdf>.

of subscription), which addressed the issues related to crimes committed through the use of new information and communication technologies. The Convention has three main sections.

1. One section is about criminal law, in which states must punish as crimes those conducts to which we referred earlier, those that appeared online and that were not provided for in our penal codes. Among them there are the illegitimate access to computer systems, the illegitimate interception of computer data, the attack on data or computer systems, the abuse of devices, the distribution of images of child pornography, and attacks on intellectual property rights. The convention, thus, presents a good starting point for those countries that wish to update their legislation.
2. A second section is dedicated to procedural law. It is proposed that the countries foresee in their prosecution systems a series of test measures designed specifically not only for the offenses provided for in the convention but, and this is very important, for any other crime committed through a computer system and to the obtaining of electronic evidence of any other crime. Rapid preservation of computer data (not the massive retention of data, but the preservation of specific data associated with a particular case), presentation of data to the judicial authorities, obtaining in real time of traffic data and content, and registration and confiscation of computer data are measures that, as we said, are not present in our procedural codes and that point to the new dynamics of cybercrimes.
3. Finally, a third section is dedicated to international cooperation, in which various assistance mechanisms are established between the states parties, with the general principle that this cooperation should be done to the best possible extent. Extradition matters are dealt with (an extradition mechanism is established between the parties for the offenses defined in the convention, to the extent that they are punished in both countries with imprisonment), mutual assistance for test measures (data preservation), data disclosure, cross-border data access and obtaining real-time traffic and content data) and spontaneous information delivery (one party can communicate to another

the information obtained from their investigations if it considers that this can help them to initiate or conclude proceedings for the offenses set forth in the convention or when such information may lead to a request for cooperation).

24.3.1 International cooperation in the fight against cybercrime

In addition to the convention, which represents an adequate tool for this type of research, there are other proposals to generate instruments of international cooperation in the fight against cybercrime. Among them, we can highlight the suggestions made by some countries in the 13th United Nations Congress on Crime Prevention and Criminal Justice[478], in relation to the need to sanction a convention of similar characteristics, but within the scope of the United Nations.

In addition, in that same congress the possibility was emphasized to use the instruments of cooperation that arise from the United Nations Convention against Transnational Organized Crime[479], This is because some cases can be considered as serious crimes committed by organized criminal groups according to the definitions stipulated in art. 2:

> "... *For the purposes of this Convention: a) "Organized criminal group" means a structured group of three or more persons that exists for a certain period of time and acts in concert for the purpose of committing one or more serious crimes or offenses established in accordance with to the present Convention with a view to obtaining, directly or indirectly, an economic benefit or other benefit of a material nature; b) "Serious offense" means conduct constituting an offense punishable by a maximum deprivation of liberty of at least four years or a more serious penalty*"

The convention includes extensive assistance mechanisms. Article 18 provides this to states parties:

478 See <http://www.un.org/es/comun/docs/?symbol=A/CONF.222/L.6>.

479 See <https://www.oas.org/juridico/mla/sp/traites/sp_traites-mla-inateram-trans.pdf>.

> *The broadest mutual legal assistance shall be provided in respect of investigations, prosecutions and judicial proceedings related to offenses covered by this Convention ... and such assistance shall also be provided when the requesting State Party has reasonable grounds to suspect that the offense referred to referenced in the sections or (b) of article 3, paragraph 1, is of a transnational nature, as well as that the victims, witnesses, proceeds, instruments or evidence of these crimes are in the requested State Party and that the crime involves the participation of a organized crime group "*

Assistance, according to that same norm, can be requested to:

> *"A) Receive testimonies or take statements from people; b) Submit judicial documents; c) Carry out inspections and seizures and liens; d) Examine objects and places; e) Provide information, evidence and expert evaluations; f) Deliver originals or certified copies of the pertinent documents and files, including public, banking and financial documentation, as well as the social or commercial documentation of mercantile companies; g) Identify or locate the proceeds of crime, property, instruments or other elements for evidentiary purposes; h) Facilitate the voluntary appearance of persons in the requesting State Party; i) Any other type of assistance authorized by the domestic law of the requested State Party "*

The same article allows to spontaneously communicate information:

> *4. Without prejudice to domestic law, the competent authorities of a State Party may, without prior request, transmit information relating to criminal matters to a competent authority in another State Party where they believe that such information could assist the authority in undertaking or successfully concluding inquiries and criminal proceedings or could result in a request formulated by the latter State Party pursuant to this Convention.*

In addition, Article 19 allows for joint investigations between several states. Among the special investigative techniques enshrined in Article 20 there is to the ability to perform, for example, electronic surveillance.

24.4 Informal cooperation mechanisms

Beyond the formal mechanisms of international cooperation to which we referred, there are other informal mechanisms that are also widely used in the research framework. These are networks of cooperation between officials and agencies that allow the exchange of information. Among them, we highlight the IberRed[480] (Ibero-American Network for International Legal Cooperation) and the G7 network 24/7[481] of high-tech crimes (G7 24/7 *Network of High Tech Crime*).

The first is a structure made up of links designated by the central authorities of the international law instruments (chancelleries, ministries of justice, etc.) and by points of contact in the judicial branches, public ministries and justice ministries of the countries that integrate it (they are the 22 countries that constitute the Ibero-American Community of Nations, as well as by the Supreme Court of Justice of Puerto Rico). Its main objective is to optimize mutual legal assistance instruments in civil and criminal matters, and strengthen ties for effective cooperation among IberRed member countries. It constitutes, thus, a fundamental tool in the conformation of an Ibero-American legal space. The communication between links and points of contact is made through a secure communication exchange platform called Iber @.

The second is designed for investigations involving electronic evidence and requiring urgent assistance from members of security forces or foreign judicial authorities, to preserve data hosted in other countries. That is why to complement (not replace) the traditional methods of obtaining legal assistance in foreign territory, the G7 has created this network as a new mechanism of contact between the member states. The protocol of the network

480 See <https://www.iberred.org/>.

481 See <https://www.oas.org/juridico/english/cyber_g8.htm>.

foresees that the police or judicial agents that need assistance from another member country communicate with their national contact point so that the latter, in turn, can process the request – if applicable – to its counterpart in the required country. The members of the network are committed to doing their best to ensure that assistance is provided as quickly as possible, within the legal framework and technical capacity of each of the countries.

24.5 Conclusions

In short, whatever the standard or platform used, what is important is that without instruments and agile tools of international cooperation, investigations can be extremely slow and even eventually fail. A similar system is planned for the member countries of the Budapest Convention.

Addressing the investigation of cybercrime requires states to adopt a legal framework that includes criminal offenses that can cover current criminal modalities, adequate procedural rules for preserving, seizing and processing electronic evidence and international cooperation agreements so that countries can effectively collaborate with each other in investigations.

TECHNOLOGICAL, REGULATORY AND SOCIAL TRANSFORMATIONS

25 Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police

Luca Belli, Pedro Augusto Francisco **and** ***Nicolo Zingales***

Abstract

This chapter argues that digital platforms are increasingly undertaking regulatory and police functions, which are traditionally considered a matter of public law. The authors emphasise that such functions have been growingly delegated to platforms by public authorities, while at the same time platforms are self-attributing such functions to avoid liability, de facto becoming private cyber-regulators and cyber-police. After highlighting the tendency towards delegation of public functions to private platforms, we provide concrete examples of such phenomenon. For example, the chapter illustrates three types of delegations of public power: the imposition of openended injunctions against innocent intermediaries, typically for content removal or website blocking; the implementation of the right to content delisting against search engines, also known as the "right to be forgotten"; and the enlisting of numerous IT companies into a voluntary scheme to counter "illegal hate speech". We show in all these cases that the amount of discretion conferred on platforms is problematic from the standpoint of the protection of individual rights. Furthermore, the paper scrutinises the case of the parallel copyright regime developed by YouTube, to emphasise another collateral effect of the privatisation of regulation and police functions: the extraterritorial application of a national legislation – US copyright, in this case – which de facto turns the platform into a private proxy for global application of national regulation. We conclude highlighting some of the challenges and viable solutions for the protection of individual rights in an era of increasing privatisation of regulation and police.

25.1 Introduction

Our analysis departs from the observation that digital platforms[482] are increasingly undertaking regulation and police functions, which have traditionally been considered a matter of public law. In particular, such functions have been growingly delegated to platforms by public regulation[483], while at the same time platforms are self-attributing such functions in order to avoid liability, de facto becoming private cyber-regulators and cyber-police. This tendency is exemplified tellingly by a series of cases we discuss in sections 2 and 3, focusing on different kinds of intermediaries, and illustrating their growing role as Internet points of control. First, we scrutinise three types of delegations of public power: the imposition of open-ended injunctions against innocent intermediaries, typically for content removal; the implementation of the right to content delisting against search engines, also known as the "right to be forgotten"; and the enlisting of a number of intermediaries into a voluntary scheme to counter "illegal hate speech". We show in all these cases that the amount of discretion conferred on platforms is problematic from the standpoint of the protection of individual rights. Second, we review the parallel copyright regime developed by YouTube, which can be deemed as the most utilised content distribution platform. This latter example is particularly useful to emphasise another collateral effect of the privatisation of regulation and police functions, which is the extraterritorial application of a national regulatory regime – in this case, US copyright legislation – de facto turning the platform into a private proxy for global application of national regulation. Lastly, we draw some conclusions, based on the presented case studies, highlighting challenges and possible solutions for the protection of individual rights in an era of increasing privatisation of regulation and police.

---

482 For purposes of this article, we rely on the definition of "platform" laid out in the DCPR Recommendations on Terms of Service and Human Rights, which refers to "any application[] allowing users to seek, impart and receive information or ideas according to the rules defined into a contractual agreement". See Belli, De Filippi and Zingales (2015), Annex 1 (n).

483 Here, the term "regulation" should be considered as encompassing both the activity of issuing rules (rulemaking) and the activity of adjudicating disputes and taking decision (ruling).

25.2 The Rise of Platforms as Points of Control

Public law and international relations are grounded on the assumption the states and international organisation are the only actors having legitimacy to elaborate and implement binding norms. In this sense, Max Weber critically influenced the evolution of domestic public law, arguing that states are the "political enterprises"[484] characterised by "the monopoly of the legitimate use of physical force within a given territory"[485] while Hans Kelsen affirmed the essential unity between state and legal order, thus considering state and law as synonyms[486]. However, these assumptions take a different flavour at the international level, where no entity may claim the monopoly of force or the legitimacy to unilaterally establish binding rules. In this context, private actors have long taken the lead and bridged the gap left by the lack of international public authority, through the institution of private ordering systems. Such systems structure[487] in a very effective fashion a wide range of variegated sectors, spanning from global finance to organised crime[488] and, of course, the online environment.

By nature, the Internet environment and particularly its application layer – which is composed of privately developed and run platforms – lends itself very well to the surge of private authority to provide law and order while avoiding conflicts of jurisdiction. Indeed, the very commercialisation of the Internet was driven by the belief that "the private sector should lead"[489] the expansion of electronic commerce over the Internet on a global basis.

Considering the above, it is not a surprise that the digital platforms that populate cyberspace have long established private mechanisms, which represent a much more efficient and reliable alternative to conflicting and ineffective public institutions in the online world. As such, the ineffectiveness of state coercion – which in the offline

484 Weber (1919).

485 Ibid.

486 Kelsen (1967).

487 Susan Strange's concept of "structural power" (Strange,1988) is useful to describe very well the capability of private entities to shape frameworks within which (natural or legal) persons relate to each other. For a discussion of how such concept can be applied to Internet intermediaries, see Horten (2016).

488 Hall and Biersteker (2002).

489 See W J Clinton and Al Gore Jr (1997).

world confers public actors a certain degree of authority and leads citizens to respect legislation – has prompted private players to replace it with the contractual rules and technical architecture that establish what behaviours are allowed in the offline world. In this perspective, digital platforms may be considered as cyberspaces in the sense of true virtual territories whose frontiers are defined by their technical architecture[490]. Notably, platform providers concentrate the capacity to unilaterally establish the law of the (cyber)land, enforce it and utilise their self-established rules to adjudicate conflicts between platform users.

First, platforms enjoy the capacity to regulate the behaviour of their users via their Terms of Service (ToS), which unilaterally establish what content users are authorised to access and share, what activities they are allowed to perform, as well as what data will be collected about users and how such data will be processed[491]. One of the salient features of platforms' ToS is that parties do not negotiate them but, on the contrary, the platform provider defines the conditions in a standard fashion – as it happens in all adhesion or boilerplate contracts – and the platform users can only decide to adhere or not to the pre-established terms[492]. In this context, the platform user is an adhering party, whose bargaining power is limited to the choice between "take it or leave it" thus giving to the ToS the force of a "law of the platform," which is established and modifiable uniquely by the platform provider. Furthermore, such quasiregulatory power may not only be exercised with regard to the definition of substantive provisions enshrined in the platform's ToS but also with regard to the criteria according to which decisions will be taken by the platform when implementing its ToS as well as the procedural and technical tools to be utilised to put into effect the platform's ToS and decisions.

Secondly, differently from legislation and, more generally, from any type of public regulation, platforms' private ordering does not need to be implemented by public executive organs. By contrast, digital platforms can directly implement their selfdefined private regulation

490 Belli (2016:202, 219).

491 See Belli & Venturini (2016).

492 See Belli & De Filippi (2012); Radin (2012); Kim (2013).

by designing the platform's technical structure according to the ToS, in a way that only allows users to perform the actions that are permitted by the platform's rules of engagement. Regulation by architecture[493] is also possible in the off-line but the level and scale of control achieved by the digital architectures of online platforms is extremely difficult to achieve even in the most authoritarian regimes of the offline world. Moreover, the algorithms that enable the platform's functionalities – for instance, establishing the order according to which information will be displayed on the platform's timeline – do not need implementation, for they are self-executing norms[494]. Platforms may also independently establish and run alternative dispute resolution and other private remedy mechanisms, as we stress in section 2.b, including by employing individuals who actively monitor users' compliance with the private regulation[495].

Thirdly, platforms usually include – and frequently impose[496] – alternative dispute resolution mechanisms to solve conflicts amongst users based on the law of the platform. As such, these intermediaries do not simply enjoy a quasi-normative power to establish the ToS and the quasi-executive power to enforce them but they also enjoy the quasi-judicial power to take decision based on the ToS provisions, for instance deliberating what constitutes "obscene" or "harmful" content. However, such private decision-making may frequently lead to erroneous decisions and over-restriction, as has been stressed by Urban, Karaganis and Schofield (2017), with regard to takedowns of supposedly illicit content.

Although the expansion of private regulation over individuals should not be considered necessarily as a negative phenomenon, the ways in which business actors exercise their "private sovereignty" should

493 In this sense, Lawrence Lessig argues that regulation of real spaces can define the constraints that real space creates and, likewise, the regulation of the cyberspaces' architecture defines constraints on cyberspaces. See Lessig (2006:127-128).

494 Belli (2016:140-144).

495 As an example, Facebook currently employs a team of more than 7,500 "community operators" dedicated to the review "millions of reports" of abusive content that Facebook receives weekly. See Mark Zuckerberg officially announcing the hiring of 3,000 extra operators to cope with the increasing reports of "abuse", on 3 May 2017, supra n. 3.

496 In this regard, a recent study conducted by the Center for Technology and Society at Fundação Getulio Vargas analysed the ToS of 50 digital platforms, demonstrating that 34% of the analysed ToS imposed arbitration as the only method for dispute resolution. See Center for Technology and Society at Fundação Getulio Vargas (2016).

be subject to public scrutiny, in order to avoid the emergence of abusive conducts. As pointed out by Chenou and Radu (2017), the rise of private authority in the online context does not necessarily result in a loss of sovereignty and decision-making power for the state, but it rather stimulates a hybridisation of governance. Indeed, it seems that the supposed efficiency of digital platforms' private enforcement is leading public actors to increasingly delegate regulatory functions to private actors. In this perspective, the OECD already stressed in 2011 the pivotal role that Internet intermediaries, such as digital platforms, play in advancing public policy objectives[497]. This consideration is leading an ample range of governments to utilise digital platforms – and Internet intermediaries in general – as proxies in order to reaffirm their national sovereignty online.

However, it should be emphasised that, in their pursuit of efficiency or compliance with national regulation, platforms end up focusing on cost minimisation and avoidance of their potential liability rather than individual rights maximisation. Moreover, the entrustment of platforms with regulatory functions tends to increase their power vis a vis market participants which depend on the platform's services, and often entrench already powerful market positions by imposing regulatory burdens on a whole category, to the disadvantage of smaller competitors. Finally, it should not be underestimated that platforms may choose to simply implement domestic legislation at the global level, rather than designing a framework better suited to meet multicultural needs and exceptions, thereby leading to the extraterritorial implementation of a discretionarily chosen regime. In the following sections, we offer some concrete examples, corroborating what we have argued above with evidence and illustrating the rise of platforms as de facto private regulators and police of cyberspace.

25.3 The Delegation of Regulatory and Police Functions to Private Intermediaries

In recent years, the above-mentioned type of delegation of public functions to online platforms has increased exponentially.

497 See OECD (2011).

As discussed, such transfer of responsibilities is grounded upon the recognition of the instrumentality of Internet intermediaries in advancing public policy objectives. This can be explained by digital platforms' essential role with regard to the circulation of information online, as well as by the inescapable need for any regulatory framework to involve platform in the implementation process, in order to be effective. However, as illustrated below, the varying mechanisms by which such involvement is established are typically lacking in the definition of limits to the platforms' discretion, thus failing to secure due respect for the fundamental rights of the individuals who bear the consequences.

Three prominent examples of this tendency are: (i) the use of injunctions against (innocent) intermediaries to remove illegal content from their properties; (ii) the entrustment of data controllers with the delisting of specific information, implementing the so called "right to be forgotten"; and (iii) the enlisting of a selected number of ICT companies for the countering of "illegal hate speech". These examples vividly illustrate that the tasks assigned to digital platforms as private executors of regulatory objectives can morph into private lawmaking and adjudication, where platforms not only choose the means of implementation of the delegated functions, but also substantially take part in the definition and interpretation of the rights and obligations of their users.

25.3.1 The Delegation of Regulatory and Police Functions to Private Intermediaries

The first example concerns a possibility that the European Union has explicitly established in its legislation concerning intellectual property enforcement[498]. Indeed, according to Article 11 of the Intellectual Property Enforcement Directive of 2004, "Member States shall [...] ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right" (IPR). The interpretation of this provision as sufficient legal basis to trigger the intermediary's duty to assist rightholders, even in the absence

498 See Husovec (2017).

of liability, was confirmed in L'Oreal v Ebay[499]. In this trademark-related case, which involved the online marketplace eBay, the European Court of Justice also clarified that such injunctions may entail the prevention of future infringements of the same kind[500]. Worryingly, the Court did not specify what would constitute an infringement of that "kind"; nor did it indicate what specific types of measures that can be imposed through such injunctions[501]. However, it provided an admonition to EU Member States that such measures must strike a "fair balance" between on the one hand, the right to intellectual property and the right to an effective remedy for the IPR holder, and on the other hand, the intermediary's freedom to conduct business and the end users' right to personal data protection, privacy and freedom of expression[502].

In a later case, the Court provided further details on the meaning of this admonition with regard to injunctions imposing website blocking. Conspicuously, such measures shall "at least partially prevent and seriously discourage the access to a targeted website"[503] but without leading to unbearable sacrifices for the intermediary in question[504] and without "unnecessarily depriv[ing] Internet users of the possibility of lawfully accessing the information available"[505]. It also established that any such measures must give the court dealing with enforcement proceedings a possibility to assess their degree of reasonableness; and must provide a possibility for Internet users to assert their rights before a court once the implementing measures taken by the Internet service provider are known[506]. Despite these important caveats, it cannot be neglected that the answers to a number of crucial questions for the effectiveness of fundamental rights protection remain subject to the discretion of the platform – or any other intermediary – implementing the measure.

499 Case C-324/09, L'Oreal v. eBay, ECLI:EU:C:2011:474, paras. 137-144.

500 Para. 144.

501 The Court only provided two examples: the suspension of the infringer, and measures that make it easier to identify customers who are operating in the course of trade. See paras. 141- 142.

502 Para. 143.

503 Case C-314/12, UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, ECLI:EU:C:2014:192. Para. 57.

504 Para. 62.

505 Para. 63.

506 Para. 57

This is especially problematic considering that the CJEU admitted[507] the possibility for courts to issue injunctions imposing an "obligation of result", as opposed to an obligation to adhere to a prescribed course of conduct ("obligation of conduct[508]"). In practice, such injunctions to obtain a particular result entail a choice between an ample range of measures with different relative impact on fundamental rights. Letting aside doubts about the suitability of such cost-benefit analysis to determining the scope of protection of fundamental rights, it is evident that economic incentives directly impact the effectiveness of protection afforded to individuals. Intermediaries are naturally inclined to err in favour of more restrictive measures, rather than to try and devise more elaborate and costly solutions that accurately balance conflicting rights: restricting access to content exhaust the demands of copyright holders, while affected subjects would need to file a separate claim in order to mitigate its adverse effects.

The trend of granting injunctive relief against innocent third party should not be considered as a European specialty and can also be noticed in other jurisdictions, notably the United States, where a number of orders have been issued requiring domain name registries, Internet service providers, payment intermediaries, search engines and social media to prevent the accessibility of infringing websites[509]. More recently, the trend was also embraced for the first time by the Canadian Supreme Court in Google v Equustek[510]. Affirming the lower court's opinion that imposed Google to delist certain trademark-infringing websites on a worldwide level, the Canadian Supreme Court found it justified to do so on the basis of its equitable jurisdiction, which among other things allows the issuing of orders against non-parties that facilitate the commission of wrongdoing[511]. Crucially, the Court

507 Id.

508 See Conde (1999:102).

509 See, e.g., Hermes v. Doe, (SDNY April 30, 2012); Chanel Inc. v. Does (D. Nev., Nov. 14, 2011); ABSCBN Corporation v Ashby, Case (Dist. Or. Aug. 8, 2014); Richemont International SA v Chen, Case (SDNY Jan. 4, 2013); Arista Records LLC v. Tkach, 122 F.Supp.3d 32 at 33-38 (SDNY 2015).

510 Google Inc. v. Equustek Solutions Inc., 2017 SCC 34.

511 Para. 31.

found "unpersuasive" Google's argument that the order clashes with the right to freedom of expression recognised in other countries, requiring it instead to prove in separate proceedings that any such conflict has actually arisen.

25.3.2 The Right to Be Forgotten and the Rise of Private Remedy Mechanisms

A second example of delegation concerns the implementation of the so called "right to be forgotten" defined by the CJEU in the Google Spain case[512]. In that case, the Court affirmed the existence of the right of all individuals to obtain erasure of their personal data from the results of search engines prompted by a search for their name, whenever such information is "inadequate, irrelevant or no longer relevant, or excessive." While the judgment has been primarily criticised for its insufficient consideration of freedom of expression, the most striking implication for our purposes is that it leaves the responsibility of implementing the aforementioned right in the hands of a private entity. Although the result of the private pondering between the accessibility and the elimination of the from the search results under an individual's name may be subsequently appealed by that data subject to the relevant data protection authority, we should stress that this mechanism creates not only one, but potentially multiple regimes of private governance running in parallel to (and possibly afoul of) the domestic legal systems.

Shortly after the ruling, all three major search engines in Europe (Google, Microsoft Bing and Yahoo) acted as de facto regulators creating a specific web form that enables users to provide the relevant information that should be delisted[513], each with their own different requirements. For example, while Google and Yahoo provide a blank space in the form for individuals to explain how the page relates to the data subject and why its content is

512 Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, ECLI:EU:C:2014:317. For a more in-depth analysis, see Zingales and Janczuck (2017).

513 According to press coverage, Google made its form available in June 2014, and Microsoft in July of the same year. It is less clear when the form first appeared on Yahoo!, although it was reported to be already in place on December 1st, 2014. See Schechner (2014); and Griffin (2014).

"unlawful, inaccurate, or outdated"[514], while Microsoft Bing poses a number of additional questions[515].

Furthermore, although these companies have not yet released any criteria they use to adjudicate conflicting rights, it is likely that significant divergence arises as a result of the open-ended character of the guidelines provided by the Article 29 Working Party[516]. The lack of prescriptions detailing the implementation of those guidelines in accordance with national freedom of expression standards, granting these entities wide discretion in the implementation of the right, is problematic for at least two reasons. First, search engines are not public courts, and thus employees tasked with making these determinations will not have the same competence and standards of professional ethics and independence that bind members of the judiciary[517]. The fact that the relevant DPA and a court may be asked to review such determinations is not sufficient to overcome this concern, as such requests are unlikely to be systematic, and can only be made by the affected data subject (not by the individual or entity who has produced the content whose accessibility is in question). Second, the nature and depth of balancing users' fundamental rights may be affected by the economic incentives and the interest of those entities to conduct their business in the most efficient and lucrative fashion. For instance, it is clear that a very probing inquiry into the circumstances of each case would impose serious costs on the search engine. Similarly, it runs against the incentives of search engines operators to publish a detailed list of their criteria for decision-making, as the availability of such criteria would make users' claims more sophisticated and more complex to decide.

514 For Google, see [accessed 31 October 2017]; for Yahoo, see [accessed 31 October 2017].

515 See [accessed 31 October 2017]. Specifically, claimants must indicate (1) whether they (and presumably anyone on behalf of whom the application is made) are public figures; and (2) whether they have or expect to have a role in the local community or more broadly that involves leadership, trust or safety. Furthermore, claimants are asked to qualify the information that Bing is requested to "block" as (a) inaccurate or false; (b) incomplete or inadequate; (c) out-of-date or no longer relevant; or (d) excessive or otherwise inappropriate. They are also invited to indicate why their "privacy interest" should outweigh the public's interest in free expression and the free availability of information. Last, but not least, they are given the opportunity to upload supporting documentation.

516 Article 29 Working Party, Guidelines on the implementation of the Court of Justice of the European Union Judgment on 'Google Spain and Inc v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzales' C-131/12., 14/EN WP 225 (26 November 2014) [accessed 1 November 2017].

517 Haber (2016).

Under these conditions, as a result of the concerns for transparency of the criteria and fairness over their substantive standards, the role of online platforms in giving effect to individual rights becomes at least questionable.

25.3.3 Countering of Illegal Hate Speech

Our third example of public functions delegation relates to the agreement defined by the European Commission in conjunction with Facebook, Microsoft, Twitter and YouTube, with the aim of adopting a specific code of conduct on "countering the spread of illegal hate speech online."[518] Above all, the code of conduct requires such companies to have in place "Rules or Community Guidelines clarifying that they prohibit the promotion of incitement to violence and hateful conduct," and "clear and effective processes to review notifications regarding illegal hate speech on their services so they can remove or disable access to such content", in the majority of cases in less than 24 hours since the reception of a valid notification. It also demands companies to "raise awareness" about their rules and procedures with users and Member States' designated national contact points, and encourages the provision of notice and flagging mechanisms to tackle hate speech with the help of experts from civil society organisations through the creation of a group of "trusted reporters". On its part, the European Commission commits, in coordination with Member States, to promote adherence to the Code to other relevant platforms and social media companies, thereby setting the conditions for this to serve as a basis for promoting greater protection against hate speech in the sector.

As pointed out by Article 19, there are significant problems of overbreadth with the definition of "hate speech" provided by the Code, which derives from the Commission's Framework Decision on Combating Certain Forms and Expressions of Racism and Xenophobia by Means of Criminal Law[519]. Notably, the code of conducts presents an overbroad focus on "incitement to hatred" (as opposed to the ICCPR's "incitement to discrimination, hostility and violence"), a lack of reference to the intent of the speaker and an unspecified threshold of seriousness for the forms of racism and

518 The text of the "Code of Conduct" agreement can be found at [accessed 31 October 2017].

519 Article 19 (2016).

xenophobia to be considered as illegal[520]. Furthermore, as noted by EDRI, the Code effectively creates a framework for privatised law-enforcement by enabling the above-mentioned companies to come up with an own definition of "hate speech" in their rules and to community guidelines, and review removal requests against those rules and guidelines[521]. Finally, there are concrete problems of oversight in the application of the Code, given that there is no direct reporting from the companies adhering to the code, but only "testing" of the reactions received by organisations that volunteered to submit notices in different Member States[522]. As a result of these tests, the review of the practices of these companies one year after the enactment of the Code revealed deficiencies in feedback provided to users submitting notification, corroborating the picture that companies enjoy a large amount of discretion both in the definition of offenses and in enforcement of those prohibitions[523].

Interestingly, the Commission has also of recent facilitated the adoption of a Common Position of national authorities within the Consumer Protection Cooperation network concerning the protection of consumers on social networks, which seemingly takes issues with the framework created by the Commission through the Code of Conduct[524]. Lamenting the "general and unspecified" nature of the criteria used by social networking platforms to refuse to display or remove content, the Position explains that contract clauses granting "unlimited and discretionary power" without identifying sufficient criteria for the suitability of user-generated content are illegal under consumer law, as they create a significant imbalance vis à vis consumers. In addition, the Position proposes the establishment of a standardised communication format between social media and consumer protection authorities including, in the case of requests for removal, information of the action taken and, if no action is taken, the legal and factual reasons for that.

520 Id., pp. 7-8.

521 McNamee (2016).

522 European Commission, 'Code of Conduct on countering illegal hate speech online: First results on implementation' (December 2016), Factsheet, [accessed 31 October 2017].

523 European Commission, 'Code of Conduct on countering illegal online hate speech 2nd monitoring', Press Release IP/17/1471, [accessed 31 October 2017], at 1 and 5.

524 European Commission, 'The European Commission and Member States consumer authorities ask social media companies to comply with EU consumer rules', Press Release IP/17/631, [accessed 31 October 2017].

While this Position constitutes a significant step towards greater accountability of social networking platforms for their removals and a model exportable to other types of digital platforms, it still does little to fix the problems originated by the vaguely worded delegation that we have described in this Section.

25.4 YouTube and iRegulate

In this Section, we consider a more specific example with regard to content regulation. Specifically, we analyse how YouTube shapes copyright through its own ToS, which are based on US copyright law, thus creating a hybrid public-private regime that is entirely privately implemented. The case of the content industry is particularly interesting, because few are the relations that are not intermediated by a third party and therefore, there is ample margin for platform action. To reach a user, the work created by an author must be fixed in some media – be it physical or digital – and subsequently distributed. In the content industry of the 20th century, these activities were typically performed by intermediaries such as big record companies, publishers and producers. These actors have been remarkably impacted by the popularisation of ICTs and by the digitisation of information. However, although digital technologies have completely changed the industry settings, such impact has not resulted in the extinction of the aforementioned intermediaries, as many thought at the end of the last century[525]. Indeed, differently from what was originally expected, the mid-2000s witnessed the emergence of streaming platforms, shifting intermediation towards the offering of content as a service, rather than as a product.

The historical reality of content industries shows that several actors who were relevant in the past still retain their importance. Although the configurations have changed, the power relations have been maintained as old intermediaries have adapted to the current scenario and big copyright holders continue to influence how copyrighted works can be reproduced and distributed. What is different now is the emergence of a new breed of actors in the content industries: the digital distribution platforms. These platforms can be characterised by their private governance,

525 In this sense, see Parker, Alstyne & Choudary (2016); Evans and Schmalensee (2016); Moazed & Johnson (2016).

consisting in privately defined rules along with the provision of an infrastructure designed to allow only the authorised interactions between the involved actors[526]. Their business models depends on the use of information and communication technologies to connect people, organisations and resources, inside ecosystems where value is generated and goods and services are exchanged. Ultimately, the goal of digital distribution platforms is to foster the establishment of agreements between their users and facilitate any type of exchange that can generate value from the distributed material.

Among these digital platforms, one of the most notable is certainly YouTube. Created in 2005 and acquired by Google just over a year later, YouTube is by far the biggest online video streaming platform in the world, with – according to its own website[527] – over a billion users, which would mean almost one-third of all Internet users. The website also states that, In the US, the platform reaches more people between 18 and 49 years old than any cable TV. YouTube has been influencing content consumption in such a way that it cannot be perceived as a mere channel between creators and consumers. As a cultural-industry intermediary, Youtube implements its own content governance technologies and imposes on its users the US Digital Millennium Copyright Act (DMCA), a legal regime that should only apply to US users – not users in any country in which a video is watched or uploaded.

YouTube's private copyright protection is enforced through two mechanisms: copyright takedowns and the Content ID system. The copyright takedown mechanism works in accordance with the DMCA. US copyright law determines that online hosting providers shall not be liable for copyright infringement if they do not have actual knowledge of the infringing material on its system, and have designated a DMCA agent to receive notifications of allegedly illegal content. Once received a notice, the online service provider wishing to escape potential liability must expeditiously take that content down. Only subsequently can the content uploader file a counter-notice, in which case Youtbe shall make that content available after 10 to 14 days, unless the original claimant demonstrates to have filed an order in court against the alleged infringer.

526 Rochet & Tirole (2003).

527 See 'YouTube in numbers' [accessed 31 October 2017].

As is well known, YouTube is a video-sharing platform which also offers users the ability to create their own channels, where they can stream or simply share with followers their own videos. Any person who believes their copyright-protected work was posted in a channel without authorisation may submit an infringement notice through a dedicated web form[528]. YouTube will remove the allegedly infringing video and the owner of the channel that uploaded it will receive a "copyright strike". According to YouTube's privately established procedure, if a channel receives three copyright strikes, its owner's account will be terminated, all their videos will be removed – importantly, even the ones that were not infringing any rights – and the user will not be able to create new accounts. After being notified that the infringing video has been struck, the owner has three possible courses of action[529]. First, the notified user can decide to wait for the strike to be removed after 90 days, subject to the condition that the user attends YouTube's "Copyright School." This means that the owner must watch an animated video explaining the functioning of copyright and answer 4 true-or-false questions about the topic to verify the content has been understood correctly.

Despite its friendliness and humour – the Copyright School video consist in a Happy Tree Friends short animation – the video has a strong message about the dangers of using copyright protected materials without authorisation, alerting the audience that infringing copyright can result in economic loss. Even though there is a short mention to the existence of fair use[530] and similar provisions in the US and other countries jurisdictions, the video is emphatic in saying that any misuse or false allegations can result in a court case[531]. The underlying message is to always use original content, despite the fact that the use of third-party content may

528 See 'Submit a Copyright takedown notice' [accessed 31 October 2017].

529 See UN Human Rights Committee.t Act'or the dissemination ofs of EU and national law. See 'Copyright Strike Basics' [accessed 31 October 2017].

530 The US Copyright Office defines fair use as the legal doctrine that promotes freedom of expression by permitting the unlicensed use of copyright-protected works in certain circumstances. Section 107 of the US Copyright Act provides the statutory framework for determining whether something is a fair use and identifies certain types of uses—such as criticism, comment, news reporting, teaching, scholarship, and research—as examples of activities that may qualify as fair use. See more at [accessed 31 October 2017].

531 See YouTube's 'Copyright School' [accessed 31 October 2017].

be legally legitimate in several cases. The second possible action is to contact directly the person who triggered the strike and ask this person to retract the claim, while the third option for the recipient of a strike is to submit a counter-notice through an ad hoc web form[532]. YouTube then forwards the counter-notice to the original claimant, who has 10 days to show proof that he or she has initiated a court action aimed at keeping the content down. Failing that, the platform will put the video back online.

The Content ID System is a more sophisticated tool. Since 2007, in order to legitimise itself as a reliable and law-abiding platform and to consolidate its position as a mainstream distribution medium, YouTube created a new system of digital identification, which can identify copyright protected materials. The system is based on the premise that any video has unique attributes that allows identification of the material even from within a short clip[533]. In this system, any copyright holder can establish a partnership with YouTube, where it uploads its protected material and allows it to become part of a reference database. YouTube can then automatically detect the use of that material in other videos. When the copyright holder establishes this type of partnership, three different actions become available to manage any further material that matches with the uploaded one. The copyright holder can decide to block a whole video from being viewed; to mute a video that contains the copyright protected music; to monetise the video by running ads against it – potentially opting for sharing the revenue with the user that uploaded the material –; and to simply track the video's statistics[534]. This gives record companies the ability to automatically monetise a mashup video that uses even a fraction of one of their owned material, or simply block that content.

In fact, much like in the case of the notice and takedown procedure implemented by YouTube, the biggest problem with the Content ID system is that it does not require the consideration

532 See Youtube's 'Counter Notification Basics' [accessed 31 October 2017].

533 See Kevin J. Delaney, 'YouTube to Test Software To Ease Licensing Fights', Wall Street Journal (12 June 2007) [accessed 31 October 2017].

534 See Youtube's'How Content ID Works' [accessed 31 October 2017].

of fair use provisions by copyright holders submitting a claim[535]. Even though the system allows for a Content ID claim dispute, the rights holder may disagree with the uploader's reasoning and request the removal of their video– which means that the potentially "fair" user will end up receiving a copyright strike. Recently, YouTube changed its Content ID policy in order to assuage at least part of these concerns. The main innovation is it will hold advertisement revenues associated with any video in a Content ID dispute, to then disburse the funds to the winning party only once the claim is resolved[536]. However, this is far from solving the problem of overbroad takedowns documented by Urban, Karagnis, Schoefield (2017).

Systems like Content ID and copyright strikes are implementations of a private right-management regime embodying a "DMCAplus" approach – i.e., voluntary, above-and-beyond enforcement measures that are undertaken by intermediaries whose compliance obligations are defined by DMCA safe harbours clauses[537]. Such regimes should not be valid outside of the US but are privately implemented by globally accessible digital platforms. This observation serves to relativise the idea that YouTube is a "global" platform, for in fact its private regulation is based on a very specific American law. Indeed, YouTube's private regulation rarely ensures respect of exceptions and limitations recognized in international copyright regimes and implemented in legislation other than US law. As discussed, although YouTube provides the possibility of a dispute between users – allowing the user that had its content blocked to defend him or herself – the mode of resolution of the conflict and the continue availability of the disputed content are at the mercy of the copyright holder[538]. In the end, through its architecture and ToS, the platform takes a clear choice of reinforcing the imbalance of power between big copyright holders and those small independent creators who depend on YouTube to make and distribute their content.

535 Note that this is in direct conflict with the Ninth Circuit's ruling in Lenz v Universal, which held that §512(c)(3)(A) (v) requires the consideration of fair use before the issuing of takedown requests. See Lenz v. Universal Music Corp., 801 F.3d 1126 (2015).

536 See Goodmann (2016).

537 See Bridy (2015).

538 Francisco & Valente (2016).

25.5 Conclusions

The examples discussed above seem to corroborate our initial hypothesis, i.e. that the advent of the Internet environment has prompted parallel consolidation of power in the hands of private intermediaries, demonstrating an increasing tendency towards the privatisation of traditionally public functions. In some instances, this tendency is the result of a specific choice taken by policymakers or courts, obliging platforms to implement appropriate responses and mechanisms to avoid liability or to give force to a decision (as in the cases of injunctions against innocent third parties and the implementation of Google Spain). In another scenario, the choice to define specific rules or to utilise specific national frameworks globally is "voluntarily" made (with different degrees of regulatory influence) by the specific platform, as shown in the implementation of the code of conduct on hate speech and in YouTube's approach to copyright exceptions and limitations. These examples illustrate that the lack of adequate constraints to platform power generates collateral damages, such as insufficient commitment to fundamental rights protection and distortion of competition in the market.

Digital platforms have become essential to allow individuals fully enjoy many of their fundamental rights, such as the right to educate themselves, their right to privacy and their freedom of communication and of information. In this sense, in light of the fact that social interactions increasingly depend on digital platforms, it is simply unacceptable for States to throw their hands up and let platform define the content, scope and limitations of fundamental rights without adequate constraints. More specifically, States cannot escape liability for violations of such rights occurring as a result of platform rules created in response to the incentives set up by the legal framework[539], be it for insufficient safeguards or for lack of regulatory intervention. International human rights law is quite clear in this respect, affirming not only "the positive obligations on States Parties to ensure human rights [and protect] individuals against acts committed by private persons or entities"[540] but also

539 Zingales (2014).

540 See UN Human Rights Committee (2004).

that "the obligations of States to respect, protect and promote human rights include the oversight of private companies."[541]

There is a spectrum of responses that States can take to ensure appropriate protection of fundamental rights, ranging from "command and control" regulation to secondary liability regimes, co-regulation, and ultimately self-regulation: thus, the encouragement of platform responsibility through commitment and transparency mechanisms constitutes the least intrusive type of regulatory intervention. Choosing this end of the scale may be preferable in the absence of evident market failures, but can only be effective in conjunction with adequate State supervision designed to ensure the detection and remedy of such failures. Additionally, targeted efforts of promotion of a culture of human rights compliance in the corporate environment may be necessary to ensure that the impacts of platforms on individuals are taken into account at the level of management as well as by shareholders, highlighting the significance of monetary consequences of human rights violations, such as reputational losses and liability under domestically implemented human rights law.

This focus on platforms' self-awareness and acceptance of their own responsibility to respect human rights is in line with the increased recognition of corporations as responsible entities for the upholding of the values of International human rights law, and should imply at a minimum that platforms do not merely devise the most cost-efficient solutions to conflicts between users, but rather strive to ensure effective protection of fundamental rights. States should remain vigilant that this does not remain an aspiration of principle, ensuring that it be given concrete effect through platforms' policies and ToS.

25.6 References

Article 19 (2016). 'EU: European Commission's Code of Conduct for Countering Illegal Hate Speech Online and the Framework Decision' (Article 19, June 2016) <https://www.article19.org/data/files/medialibrary/38430/EU-Codeof-conduct-analysis-FINAL.pdf> Acesso em: 31 out. 2017.

Article 29 Working Party, 'Guidelines on the implementation of the Court of Justice of the European Union Judgment on 'Google Spain and Inc v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzales' C-131/12', 14/EN WP 225 (26 de novembro, 2014) Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion recommendation/files/2014/wp225_en.pdf>. Acesso em 1 nov. 2017.

541 See CoE Recommendation CM/Rec (2014)6.

Belli, L. (2016). De la gouvernance à la régulation de l'Internet. Berger-Levrault.

Belli L, De Filippi P and Zingales N (eds.) (2015). 'Recommendations on terms of service & human rights. Outcome Document n°1. Disponível em:<https://tinyurl.com/toshr2015>. Acesso em: 31 out. 2017.

Belli L & Venturini J (2016). 'Private ordering and the rise of terms of service as cyber-regulation' (2016) 5 (4) Internet Policy Review.

Bridy A (2015). 'Copyright's Digital Deputies: DMCA-Plus Enforcement by Internet Intermediaries'. J A Rothchild (ed.), Research Handbook on Electronic Commerce Law (Edward Elgar, 2016).

Center for Technology and Society at Fundação Getulio Vargas (2016). 'Terms of Service and Human Rights: An Analysis of Platform Contracts' (Revan Press, 2016) Disponível em: <http://tinyurl.com/toshr>. Acesso em: 31 out. 2017.

Chenou J M and Radu R (2017). 'The "Right to Be Forgotten": Negotiating Public and Private Ordering in the European Union' Business & Society.

Evans D and Schmalensee R (2016). Matchmakers: The New Economics of Multisided Platforms. (Harvard Business Review Press, 2016)

European Commission, 'Code of Conduct on countering illegal hate speech online: First results on implementation' (Dezembro, 2016), Factsheet, <http://ec.europa.eu/information_society/newsroom/image/document/2016-50/factsheet-code-conduct-8_40573.pdf>. Acesso em: 31 out. 2017.

European Commission, 'Code of Conduct on countering illegal online hate speech 2nd monitoring', Press Release IP/17/1471. Disponível em: <http://europa.eu/rapid/press-release_MEMO-17-1472_en.htm>. Acesso em: 31 out. 2017.

European Commission, 'The European Commission and Member States consumer authorities ask social media companies to comply with EU consumer rules', Press Release IP/17/631. Disponível em: <http://europa.eu/rapid/press-release_IP-17-631_en.htm>. Acesso em: 31 out. 2017.

Francisco P and Valente M (2016). Da Rádio ao Streaming: ECAD, Direito Autoral e Música no Brasil. (Azougue, 2016).

Griffin A (2014). 'Microsoft's Bing and Yahoo search engines have started to fulfill the controversial requests', The Independent (Londres, 1º de dezembro, 2014). Disponível em: <http://www.independent.co.uk/life-style/gadgets-and-tech/news/microsoft-and-yahoo-join-google-in-deleting-search-results-under-right-to-be-forgotten-ruling-9896100.html>. Acesso em: 31 out. 2017.

Goodmann D (2016). 'YouTube's Content ID Policy Change Now Saves Lost Monetization for Fair Use Videos' (Washington Journal of Law, Technology and Law Blog, 1º de dezembro 2016). Disponível em: <https://wjlta.com/2016/12/01/youtubes-content-id-policy-change-now-saves-lost-monetization-for-fair-use-videos/>. Acesso em: 31 out. 2017.

Haber E (2016). 'Privatization of the Judiciary' (2016), 40 Seattle University Law Review 115.

Hall RB, and Biersteker TJ (Eds.) (2002). The emergence of private authority in global governance. (Cambridge University Press, 2002).

Horten M (2016). Closing of the Net (Polity Press, 2016).

Husovec M (2017). Injunctions against Intermediaries in the European Union. (Cambridge University Press, 2017).

Kelsen H (1967). Pure Theory of Law. Translation from the Second German Edition by Max Knight. (University of California Press, 1967).

Kim NS (2013). Wrap Contracts: Foundations and Ramifications (Oxford University Press, 2013).

OECD (2011). The Role of Internet Intermediaries in Advancing Public Policy Objectives (OECD Publishing, 2011). Disponível em: <http://dx.doi.org/10.1787/9789264115644-en>. Acesso em: 31 out. 2017.

McNamee J (2016). 'Guide to the Code of Conduct on Hate Speech' (EDRi, junho, 2016). Disponível em: <https://edri.org/guide-code-conduct-hate-speech/>. Acesso em: 31 out. 2017.

Moazed A and Johnson N (2016). Modern Monopolies: What it Takes to Dominate the 21st Century Economy (St. Martin's Press, 2016).

Parker G, Alstyne M and Choudary S (2016). Platform Revolution – How Networked Markets Are Transforming the Economy – and How to Make Them Work for You (W. W. Norton & Company, 2016).

Radin M J (2012). Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law (Princeton University Press, 2012).

Rochet J C and Tirole J (2003). 'Platform Competition in Two-Sided Markets' (2003) 1 (4) Journal of the European Economic Association 990.

Schechner S (2014).'Google Starts Removing Search Results Under Europe's 'Right to be Forgotten'', Wall Street Journal (New York, 26 de junho, 2014). Disponível em: <https://www.wsj.com/articles/google-starts-removing-search-results-under-europes-right-to-be-forgotten-1403774023>. Acesso em: 31 out. 2017.

Strange S (1988). States and markets (Continuum, 1988).

UN Human Rights Committee (2004). General Comment 31/2004. Nature of the General Legal Obligation on States Parties to the Covenant. CCPR/C/21/Rev.1/Add.13. Disponível em: <http://www.unhcr.org/4963237716.pdf>. Acesso em: 11 nov. 2018.

Urban JM, Karaganis J and Schofield BL (2017). 'Notice and Takedown in Everyday Practice' UC Berkeley Public Law Research Paper No. 2755628. Disponível em: <https://ssrn.com/abstract=2755628>. Acesso em: 31 out. 2017.

Weber M (1919). 'Politics as a Vocation'. in H H Gerth and C Wright Mills (eds.) From Max Weber: Essays in Sociology (Routledge & Kegan Paul, 1948).

Zingales N (2014). 'Virtues and perils of anonymity: should intermediaries bear the burden? '(2014)' 5 (3) Journal of Intellectual Property, Information Technology and E-commerce 155.

Zingales N and Janczuck A (2017). 'Implementing the Right To Be Forgotten: towards a co-regulatory solution?' e-conférence on the Right to Be Forgotten in Europe and Beyond, Maio, 2017, Blogdroiteuropeen. Disponível em: <http://wp.me/p6OBGR-22t>. Acesso em: 31 out. 2017.

26 Building the Future of the Internet with our Youth Voices

Sebastian Bellagamba and *Raquel Gatto*

Abstract

The purpose of this work is to present the challenges and opportunities that users, communities and societies will face in the immediate future, using the Paths to Our Digital Future report, launched in 2017 by the Internet Society. This analysis was based on forecasts about the future of the Internet taken from a wide range of sectors, and among the set of recommendations derived from the contributions received, the article focused on one of them: training and the empowerment of young people. This topic, which is gaining more and more space in the discussions on digital policies, is approached through an analysis of documents and statements that deal with the participation of digital natives, and points out the need to raise awareness among youth and that is actively involved in the processes of Internet Governance.

26.1 Introduction

"Inter-networking"[542] is a phenomenon that permeates our daily lives. It is a tool used by many individual users and businesses. It is the news vehicle in real time. It is the key to social and political movements. It is many things at once, and allows others to scale, expand, transform and be much more. It is also what is generally called the Internet.

Despite the fact that the Internet has been a powerful catalyst for change, continuously nourishing and remodeling the current information society, it is important to note that it has also been a very recent phenomenon. There is still a wide range of issues that must be adequately addressed in relation to their social, legal, political and technological impacts. In order to get solid answers to these global questions, we need to have a wide range of experts and interests that can participate meaningfully in the discussion

542 See Cerf, Dalal and Sunshine (1974).

and contribute to the development of the best possible outcome. To be truly open and inclusive, that collaborative effort must also include the young participants, the next generation that is shaping our digital future.

26.2 Steps towards our digital future

In 2017, Internet Society[543] celebrated its 25 years, which leads us to look back to the lessons learned in the way of the defense of an open, global, interoperable, resistant and reliable Internet[544]. It also provides the opportunity to look ahead and reflect on the future of the Internet, and what will be the challenges to continue advocating for basic principles and the Internet for everyone, everywhere.

Retaking this challenge, the Global Internet Report entitled "Pathways to our digital future", presented in September 2017, shows the work of 18 months to gather predictions about the future of the Internet from a wide range of stakeholders, and identify the forces of change that will bring us closer or will take us away from the Internet that we want to have in 5-10 years. In addition, depending on the possible scenarios, the study has also presented key recommendations that we believe we should all adopt to guarantee this vision of the future.

Among the forces of change identified, there are no surprises when we consider that factors such as the evolution of Artificial Intelligence, the Internet of Things, the Internet Economy and Cyber Threats play a key role in the future of the Internet. However, there is a sense of uncertainty as to the direction it will take to address such issues, such as what is the most appropriate role for governments and what should be the most relevant regulatory reaction to these new challenges. In addition, areas of impact have been identified in the user's ability to connect, speak and share, as well as ability to innovate, choose and trust will be affected by the drivers of change. Figure 1 below illustrates the key findings of the study mentioned above.

543 View <http://internetsociety.org/>.

544 See ISOC (2016).

Figure 1: Impulsores da mudança e áreas de impacto para a Internet do futuro (GIR 2017, ISOC)

Both the elements that drive change as well as the areas of impact highlight the challenges and opportunities that users, communities and societies will face in the immediate future.

Many respondents have expressed their firm belief in the potential of the Internet to continue to drive innovation in order to generate a positive change in the lives and benefits of people in education, health, economic prosperity and social change. However, these hopes and beliefs are counteracted by far-reaching fears that the Internet may be seen and used differently in the future. For example, there is a concern that some interested parties will try restrict the freedoms of the Internet through centralization, mass surveillance and stimulating fragmentation.

In this line, some respondents are concerned about the threat of new divisions and how these will not only deepen the existing disparities between people in a given society, but also between

countries that broaden the gap between the developed world and the developing world. In particular, the report explores the emergence of a new security and trust gap characterized by cyber threats that continue to multiply, and a growing gap between security conscious users and those lacking the skills, knowledge and resources to protect themselves online.

Therefore, taking into account the need for a way forward to address these challenges, the report presents a set of recommendations derived from the contributions received. Based on this, politicians, technologists, entrepreneurs and activists can act to ensure that the future Internet remains user-centered, that it defends and reaffirms our freedoms and rights and that it strives to work for the benefit of all.

1. Human values must promote the development and use
2. Apply human rights online and offline

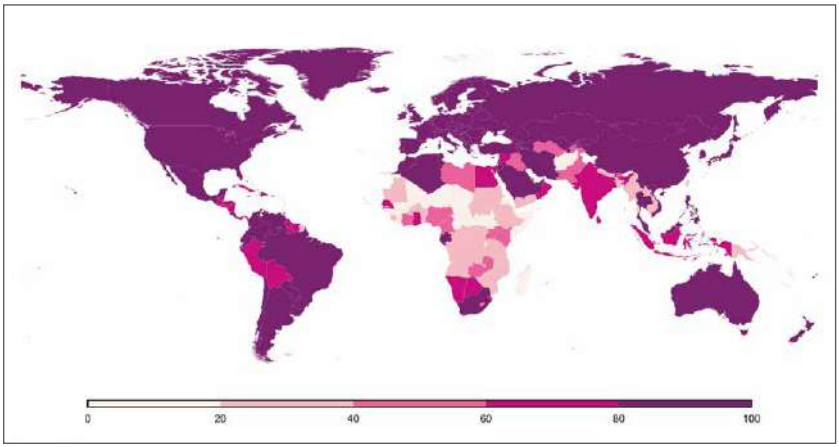


Figure 2: Proportion of young people (15-24) using the Internet (ITU Facts and Figures 2017)[545]

3. Put the interests of the users first with respect to their own data
4. Act now to close the digital gaps
5. Making the Internet economy work for everyone
6. Adopt a collaborative approach to security
7. Increase the responsibility of those who handle the data

545 ITU (2017).

8. Build strong, secure and resilient networks

9. Address the need for rules of social behavior online

10. Empower people to shape their own future

26.3 Bringing the voice of the new generation

Half of the population worldwide now has access to the Internet[546]. However, it is more impressive to realize that, currently, around 70% of young people between the ages of 15 and 24 are connected to the Internet.

These young citizens are not only the so-called "digital natives", who were born with existence and grew up using the Internet since childhood; they are the ones who should have a voice to shape the use of this communication tool and to promote the future of the Internet.

In corroborating this vision, the Geneva Declaration (2003) of the first phase of the World Summit on the Information Society (WSIS) has clearly recognized that:

> *-11. We are committed to materialize our common vision of the information society, for us and future generations. We recognize that young people are the future workforce and leading creators and earliest adopters of ICTs. They must therefore be empowered as learners, developers, contributors, entrepreneurs and decision-makers. We must focus especially on young people who have not yet had the possibility to take full advantage of the opportunities offered by ICT. We are also committed to ensuring that, in the development of applications and the exploitation of ICT Services, children´s right and well being are respected and protected ."*[547]

In that regard, the need to provide training and empower young voices has been reinforced by the Tunis Commitment (2005), in its

546 See <http://www.internetlivestats.com/internet-users/>.

547 Declaration of Geneva issued on December 12, 2003, within the first phase of the World Summit on the Information Society, document available at: <https://www.itu.int/net/wsis/docs/geneva/official/dop.html>.

paragraph 25[548] and by the NetMundial Multipartition Declaration (2014)[549].

Therefore, it is widely recognized that young people should know and actively participate in Internet Governance processes, in order to have the opportunity to shape public policies that will affect us all.

Bearing this in mind, it is necessary that there be concentrated and solid efforts to: (i) develop and promote capacity development programs aimed at young people, such as the South School of Internet Governance[550] which celebrates its tenth anniversary; (ii) adopt flexible and dynamic processes to involve and build the community for young citizens, such as the Internet Society's Youth Special Interest Group[551]; and (iii) implement mechanisms for the meaningful participation of all stakeholders, including young people, such as the growing initiatives for youth-led IGFs (eg LAC Youth IGF[552], Asia Youth IGF[553]).

26.4 Final Considerations

The future is uncertain for all of us. But we can still take steps to ensure that it is forming in the direction we want. The Internet is a powerful tool, which must be global, open and secure. And because we live in an interdependent world, decisions about the future of the Internet must be inclusive and multi-stakeholder. Your future will not only be defined by the new technologies that will continue to emerge, but also by empowering people and putting them at the center of political decisions. We can build a beneficial future for the Internet, together.

---

548 *.25 We reaffirm our commitment to empower young people as key contributors to build an inclusive information society. We will actively engage young people in innovative ICT-based development programs and expand opportunities for young people to participate in e-strategy processes".* Commitment of Tunisia issued on November 18, 2005, during the second phase of the WSIS, available at: <https://www.itu.int/net/wsis/docs2/tunis/off/7.html>.

549 *"Enabling meaningful participation: Anyone affected by an Internet governance process should be able to participate in that process. Particularly, Internet governance institutions and processes should support capacity building for newcomers, especially stakeholders from developing countries and underrepresented groups".* NETMundial Multistakeholder Declaration, published on April 24, 2014 in São Paulo, Brazil. Document available in: <http://netmundial.br/wp- content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>.

550 See <http://www.gobernanzainternet.org/ssig2018/>.

551 See <http://obdjuv.org>.

552 See <https://youthlacigf.com>.

553 See <http://yigf.asia>.

26.5 References

Cerf V., Dalal Y., Sunshine C. (1974). Specification of Internet Transmission Control Program, Request for Comment 675. <https://tools.ietf.org/html/rfc675>.

Internet Society (ISOC) (2016). Policy Brief: Internet Invariants. <https://www.internetsociety.org/policybriefs/internetinvariants>.

Internet Society (ISOC) (2017). Paths to our Digital Future. Global Internet Report entitled. <https://future.internetsociety.org>.

Unión Internacional de Telecomunicaciones (UIT) (2017). ITU Facts and Figures 2017. <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf>.

27 Disruptive Technologies and their Impacts for Latin America

Vanda Scartezini

Abstract

Disruptive technologies are responsible for the most important evolutions in humanity. The main revolutions in development were all linked to the disruptive technologies of their times. Based on the Internet, new technologies have impact in society. It is about the exploitation of what will or will not be relevant in the near future. These discussions are being developed in various forums around the world and this text explores a subset of interest within the context of Internet Governance. In particular, some points of relevance for our region are raised, as discussions and alerts for our governments in relation to measures that need to be put into practice to guarantee the development of our nations and the economic and social future of the new generations.

27.1 Introduction

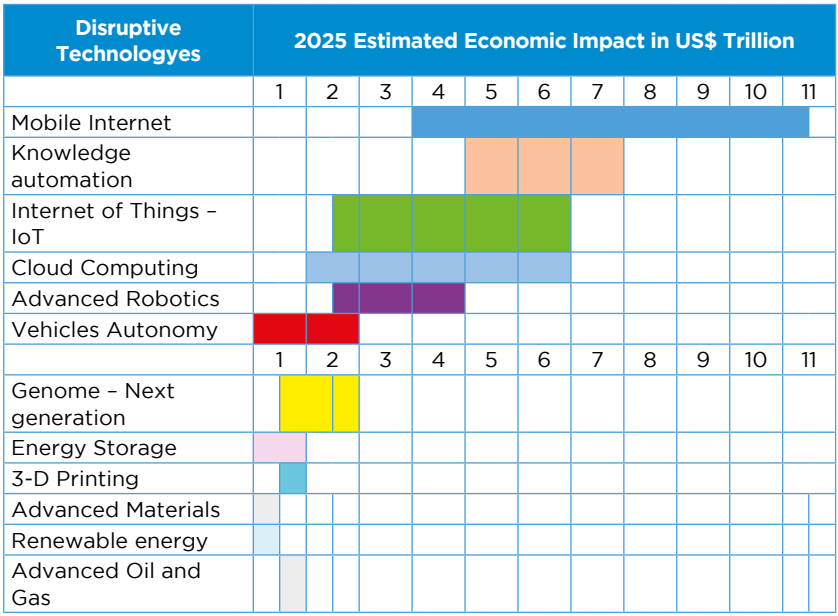
Although Internet Governance is extremely broad, discussing points ranging from social issues to high technology, all areas of discussion have a common point, which refers to the best and most optimized use of the Internet for the well-being and improvement of the quality of life of all users.

In this sense, Disruptive Technologies do not differ from this approach, promoting its aspects in Internet Governance. What leads to a technology to be considered disruptive can be defined in several ways, but a good definition is that made by McKinsey Global Institute: “Progress that will transform life, business and the economy globally.”

Most new technologies when they appear, usually earn, immediately, the title of “the next big change,” but most do not generate this impact because they do not have the essential characteristics of scalability, cost and impact on society in general.

Some technologies can be clearly understood as disruptive today, although they were not considered so in their early stages, such as the Internet itself, which brought profound impacts on society, on the way of acting, on interaction with the other, living or machine, and on the management of one's own life.

McKinsey's study analyzes some of the most recent technologies considered disruptive and calculates their financial impact based on market impact and economic potential without considering gross domestic products or profits. Figure 1, below, shows this result, revealing a possible range of impact of each of the technologies that they consider to have disruptive potential. McKinsey estimates that together, these technologies will have a potential economic impact between US $ 14 to 33 billion per year in 2025.



Source: Author's elaboration

Although we should agree with many of the technologies identified in the McKinsey study, some are from fields not directly connected to the Internet, losing their value for the focus of this article, within the framework of Internet Governance. However, in this same analysis we see that the technologies with the greatest economic

potential are in the field of Information Technology and Internet, although they demand solutions in other fields of engineering. These are mobile Internet, knowledge automation, IoT, cloud computing, advanced robotics and autonomous vehicles.

Most of these technologies are known and we already have, individually, the conviction that they cause growing impacts, we can therefore consider them as having disruptive potential. We also know that there is a relevant interaction between different technologies and that the genome, for example, has only been viable and will be viable in its new generation, as a disruptive technology, depending on the existence of the Internet itself: the sequencing of the human Genome (2006) was possible, for example, by the use of thousands of networked computers distributed around the world. Several groups that today study the genome are part of universities, such as the MIT (Massachusetts Institute of Technology), with a history of successful research in Information and Communication Technologies. Autonomous vehicles, totally dependent on software and the Internet, will also depend on the evolution of energy storage solutions and alternative energies, due to the enormous impact they will have on the countries' energy consumption.

Among the various technologies that stand out as disruptive, Knowledge Automation, for its economic impact on general productivity and education, deserves special attention, mainly by policymakers, seeking the best use in their countries.

At the last meeting of the Internet Governance Forum, IGF, organized in December 2017, Professor Divina Frau-Meigs, from the Sorbonne Nouvelle, raised the issue of the impact that new technologies will have on learning, highlighting the importance of the new types of literacy (digital literacies, for electronic media for example) and in the preparation of populations, an important discussion that is imposed on future employability and training of populations for the new reality.

It is of our interest, in the sphere of Internet Governance, also to understand how technologies that are being deployed will have their role in the development of the Internet and in the expansion of the Internet of Things (IoT), or as new protocols are going to interact with existing systems such as the Domain Name System (DNS).

27.2 Disruptive technologies and the domain name system

Blockchain, by itself, can be a disruptive technology, being the technological translation of any safe process, generating infinite possibilities for applications that can modify the way they are seen, understood and treated today. Today Blockchain is basically being used for the viability of "assets", which although not financial, have market value, such as "bitcoins" or cryptoassets.

The forecast is that Blockchain will flood the industry, logistics, services and all activities where there is a process to follow, a process which demands security to be effective. Although there are studies on issues that may affect its global impact capacity, such as the fixed rate of block addition, recovery limitations and even too much transparency, which may be a limitation in some applications, the diversification of Blockchain applications has been growing exponentially. If its impact will be enough to justify it as a disruptive technology, only the future can say.

Meanwhile, several new technologies are being tested, seeking to facilitate the expansion of Blockchain itself. One of them is the "Handle System"[554]. Developed for use in administration, it is an implementation of the identifier / resolution component of the Digital Object Architecture (DO Architeture). Some examples of use of the Handle System include document management, control within the supply chain, financial security, data set identification in big data processing and resolution systems in Blockchain technology. Also on this point another study suggests that because the Dona Foundation, owner of the technology, is a closed entity, the documentation can be lost if the foundation ceases to exist, and with this possible loss, the possibility of evolution would be impaired. But they are market speculations and, again, the future will tell about the real success of this technology.

Ethereum, (today known more as the crypto-active "ether" and the Blockchain) opened a new project ENS – Ethereum Name Service that, according to its creators, is a new, safe and decentralized way

554 See <https://www.dona.net/handle_system/>.

to direct resources, both incoming and outgoing of Blockchain, using simple names easily read by humans. Actually, it is a decentralized Registry, where anyone can create names with the suffix 'eth', as today is usually done with the names of Internet Domain in the DNS industry.

ICANN is getting involved in the OX Project, which focuses on enhancing decentralized exchanges between tokens (digital contracts used in cryptocurrency exchanges / "cryptocurrencies"). The OX project is open to the community.

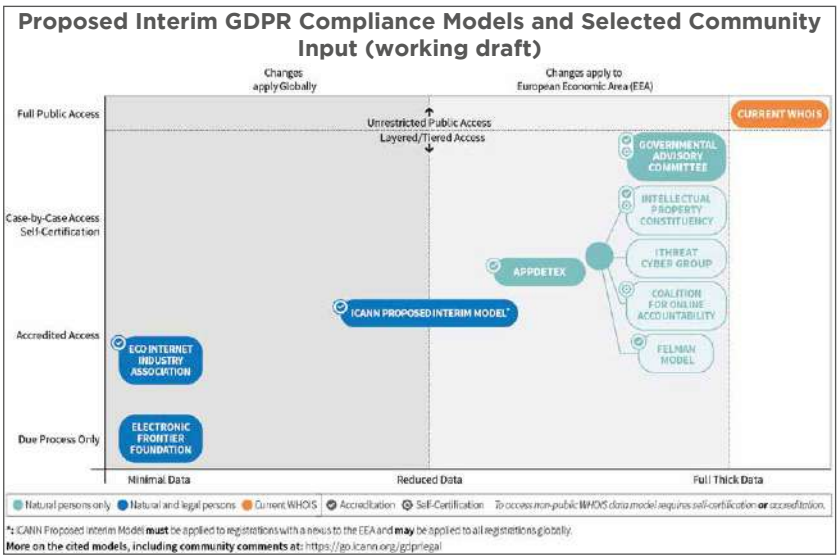
In relation with the DNS evolution, with focus on the IoT (Internet of Things) environment, the AfNIC Labs is working on two different ecosystems: one hierarchical and one at the same level ("flat") which is based on an evolutionary vision for implementations in supply chains. In the IoT environment, in the hierarchical routing and Based on cluster, each network node has a different role. In this architecture, higher energy nodes can be used to process and send information. This means that the creation of clusters and the assignment of special tasks to the cluster headers can contribute greatly to the overall scalability of the system, lifetime and energy efficiency. In flat routing all network nodes execute the same functions and processes. In these networks, each sensor node collaborates together to perform the detection task, and it is not possible to assign a global identifier to each node.

27.3 How, when and where is the disruption happening?

It is important to highlight other points that are discussed by society in various forums on the impact of disruptive technologies: a question is about the "when and how" Internet users should interact with these complex systems and how society must prepare, so there is no interference neither too early nor too late.

Another point always raised is the discussion of privacy, which is gaining a lot of space, mainly after the regulation of the Protection of Personal Data by the European Union (General Data Protection Regulation GDPR) which, in principle, affects all who reside, or have businesses in Europe, with companies or individuals, such as the commercialization of Internet Domain Names. One of the

points of relevance in this discussion, by the global market form, is the identifiers used for the acquisition, anywhere in the world, of domain names. As a manager of names and addresses on the Internet, ICANN proposed a model for the debate, in relation to this identifier, WHOIS and compliance with the GDPR, which is shown in Figure 2[555].



Source: ICANN

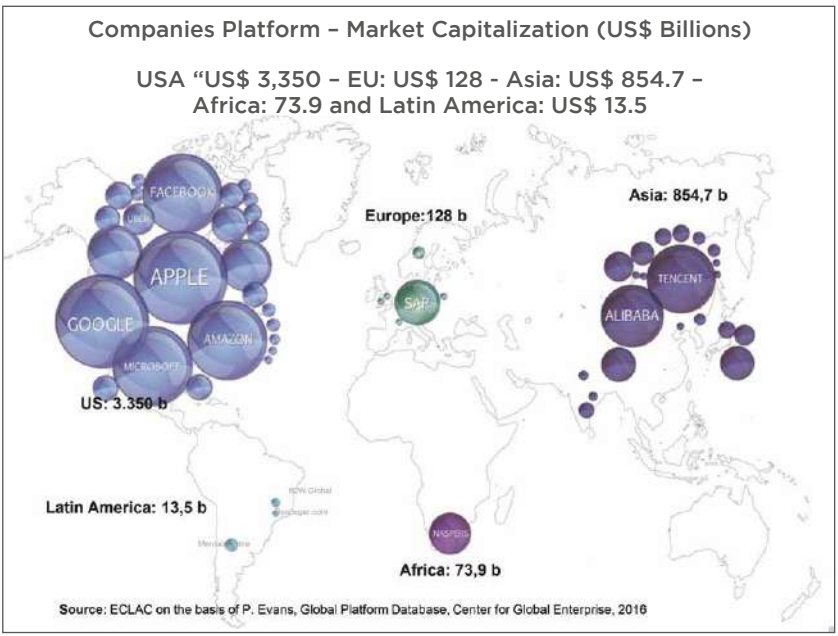
They are all points without a definitive answer and they must be in the discussion tables together with society.

When we take the discussion to Latin America, the main focus is on technologies that have an impact on society, such as the evolution of knowledge automation and the inexorable arrival of new generations of robotics, which will consequently lead to the reduction of employability existing in the region.

A study by ECLAC (Castillo, 2016), shown in figure 3, shows the concentration of "platform companies" in the United States and Asia and a few examples, on a much smaller scale, in Latin America, showing that our societies are not focusing on the economic impact that these companies, called platforms, generate

555 More details can be found in <https://go.icann.org/gdprlegal>.

for their countries. Even Africa presents at least one impressive business solution, Naspers, a company from South Africa, dealing with Internet and digital media, already present in 130 countries. In Latin America, with our 0.4% share, we have three outstanding companies: Despegar.com; Mercado Libre and B2W group.

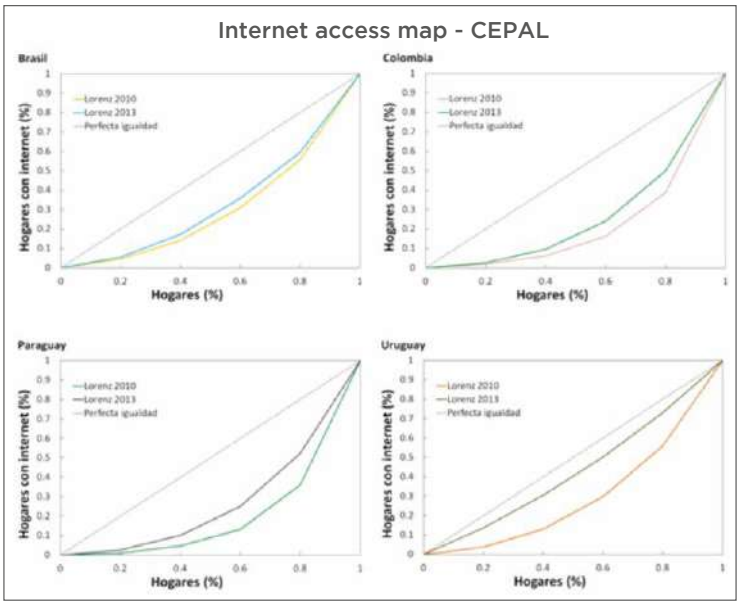


Source: EclaC in the bases of Evans (2016).

The map of Internet access in Latin America, from ECLAC itself, based on the national statistics of the different countries, gives us a vision of the necessary effort for effective participation, both economic and social, in the populations of our region, against the results that new disruptive technologies bring to markets. Studies carried out already in 2015 by the IDB (Inter-American Development Bank) proposed policies that would help countries in the training of their populations to face challenges of new technological environments, even with tools such as the Skills Bank[556]. SkillsBank is an online database that adds evidence on policies for the development of skills throughout the life cycle of citizens, which can be used by governments to measure the effectiveness of policies implemented in their countries, which can

556 See <https://skillsbank.iadb.org/>.

be a basis for adjustments in existing policies or the implementation of new ones, based on the evidence collected. Actions such as continuous training and professional reorientation, as well as better preparation of the new generations for a society in constant change in their demands of ability, need to be addressed with more priority by the governments of the countries of our region.



Source: CEPAL.

In a specific study, ECLAC recommended that Latin American countries "promote the exploitation of cryptocurrencies" with the objective of "adapting to financial technology and becoming a pillar for the region in this field."

It is interesting to note that the so-called digital currencies are not currencies, they are assets that, as they reside in Blockchain bases, would stimulate the understanding and use of new applications of this technology and new innovative businesses could arise from this knowledge. The analysis of ECLAC takes into account the difficulties of infrastructure and regional payment methods, where the use of these cryptocurrencies could help the region increase its participation in the digital economy; for example in electronic commerce, or even in access to savings or loans, suggesting that

the region adopt as a legal framework the model adopted by the United Kingdom to prevent fraud, also referring to other legislations in different countries. In this same study, ECLAC cites existing information in the CARICOM region[557] within the framework of the United Nations Convention on the Safety and Protection of the Rights of Persons with Disabilities.

Other countries, such as Brazil, with more strengthened banking systems, digitized and accessible by the majority of the population, have been facing resistance to better organizing coexistence with cryptocurrencies.

27.4 Conclusions

Finally, it is interesting to highlight the vision of the World Economic Forum (WEF 2015) about when each technology will be really dominant in the markets. Figure 5, below, presents the results of the survey conducted with 800 technology executives and experts from the Information and Communication Technologies sector, highlighting when the indicated technologies could have the greatest impact in the sector.

When will the future come? (Source: WEF 2015[558])

2018	2021	2022	2023	2024	2025	2026	2027
Storage for all (cloud)	Robots and services	IoT Clothes connects to Internet 3D printing and manufacturing	Implantable technologies Big data in decisions New interfaces vision Digital Presence Governments + Blockchain Super mobile computers	Ubiquitous computing Human Organs in 3D Connected House	3 D in Consumer items At the Council of the companies	Autonomous Autos On executive levels of the companies	Bitcoins and Block-chain

Figure 5 (Note: AI – Artificial Intelligence in English).

Stakeholders and, in particular, policy makers in the Latin America region, should be attentive to the differences existing in relation to

557 View <http://www.caricom.org/>.

558 WEF (2015).

the other regions, so as not to hinder the growth and welfare of their populations, with the domination of the technologies that are, in fact, intended to modify the structure of societies and the economy.

Not participating in these changes leads to losing relevance in the world stage. A relevant example of the importance of adhering to the first moments of a technology to appropriate it for the benefit of its populations, is epitomized in the Internet itself. In our Latin American and Caribbean region most of the countries joined the Internet immediately, in the 80s, receiving from Jon Postel their country code (country code: .ar; .br; .cl; .mx etc.) making possible the expansion of their internal networks and offering the opportunity of participation in the digital world to its populations through economic and social growth. The volume of Internet users in our region is today the result of this pioneering movement of the past. With a population of 625 million estimated in 2015, 54.5% were already Internet users and although there is more concentration in the cities and less participation in the rural regions, it is in any way a relevant percentage.

Why do we not have the same proactive stance in relation to these new movements?

27.5 References

Castillo M. (2016). Tecnologías disruptivas en la era digital. Comisión Económica para América Latina (CEPAL). <https://www.cepal.org/sites/default/files/events/files/01_mario_castillo_-_tecnologias_disruptivas_en_la_era_digital.pdf>.

Evans P. (2016). Global Platform Database. Center of Global Enterprise.

Manyika J., Chui M., Bughin J., Dobbs R., Bisson P, and Marr A. (2013) Disruptive technologies: Advances that will transform life, business, and the global economy. McKinsey Global Institute.

WEF. (September 2015). Technology Tipping Points and Societal Impact. Survey Report. <http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf>.

28 Regulatory Perspective of Artificial Intelligence

Jorge J. Vega-Iracelay

"Frans wanted to recreate biological evolution on a digital level. He worked with self-taught algorithms, algorithms that through the trial and error method can improve themselves[559]."

Note: The author highlights and appreciates the collaboration of Professor Alejandro Martínez Ramos in the research and editing of this article.

Abstract

The growing development of applications and solutions of artificial intelligence, brings many questions about the way in which this phenomenon will impact our lives, our interaction with machines and computers; and even, the interaction between human beings themselves. This brief essay addresses some of the challenges posed by artificial intelligence, and suggests certain regulatory parameters to address them from a legal perspective.

28.1 Introduction

The followers of the successful saga of "Millenium", created by the Swede Stieg Larsson, will know immediately what I'm talking about. In the fourth installment of the series, Mikael Blomkvist and Lisbeth Salander investigate the murder of Frans Balder, a scientist who presumably would have made artificial intelligence move from devices and systems programmed by humans, to a higher stage in which it is capable of understanding their own existence, evolving and creating new forms of intelligence. That happens in the distant fiction of Millenium. On the other hand, artificial intelligence has been a dream for many since Alan Turing wrote in the 1950s his document called "Machinery and Intelligence Computer[560]".

559 In "What does not kill you makes you stronger" *(Millenium 4)*, by David Lagercrantz; published in Spanish by the publisher Planeta (Destino, Colección Áncora y Delfín), with the translation by Martin Lexell and Juan José Ortega. The quotation corresponds to chapter 13, specifically at the moment when Farah Sharif -wife of Frans Balder- explains to Mikael Blomkvist Balder's work on artificial intelligence.

560 Turing (2009).

However, in the immediate reality – even with all proportion kept – there are already signs of this phenomenon[561]. Although developers have been teaching computers to see, hear, speak and understand human beings for decades, which represents implementations of Artificial Intelligence, their current development and scope are exponential at present given the enormous amount of information (Big Data) available, combined with its processing and storage by the cloud computing.

The artificial intelligence that we have usually known so far is essentially a way of *"Machine learning"*, in which a computer can react to external stimulation from information provided in advance, and have the capacity to improve its response – according to human expectation – based on the increase and analysis of information derived from its interaction with such stimuli external. In other words, there is Artificial Intelligence when a machine or a computer system imitates the cognitive functions that human beings associate with other human minds, such as learning, analyzing information, and solving problems.

Some examples of this form of intelligence occur in our mobile phones, like their assistants providing information, following instructions, facilitating tasks or predicting activities based on preferences; in cars, for parking or driving autonomously; or in innumerable computer solutions, to analyze large volumes of information and execute tasks based on their results.

To implement these tasks, human intervention seems obvious and necessary. The phenomenon to which I refer, however, modifies this premise: although it does not necessarily dispense with human interaction, it is the artificial intelligence system itself that is capable of creating new forms of intelligence – even for new purposes – or of taking advantage of knowledge or discern issues that we have traditionally considered unique, unrepeatable and of the human being; for example, the value judgments, the weightings between two or more alternatives, or in general the decision making based

561 For example, in May 2017 various specialized media and even general information newspapers echoed the advances published by Google of its AutoML program -in essence, aimed at allowing an artificial intelligence system to create another system, without human intervention, with characteristics superior to the first.

on an imprecise combination of sensory information, data, purpose, emotions and interests.

This type of intelligence – which is usually referred to by various names, such as super artificial intelligence, *Human Level Machine Intelligence* or supra-human intelligence, among others – is essentially the technological singularity to which Vernor Vinge refers in his well-known work *"The Coming Technological Singularity: How to Survive in the Post-Human Era*[562]*"*, undoubtedly one of the most frequently cited essays when dealing with aspects and perspectives of artificial intelligence.

According to Vinge, no later than the third decade of this century, there will be forms of supra-human intelligence that will modify essential aspects of nature as we know it; for example, it anticipates that biotechnological developments will be able to alter the characteristics of the species, and that the changes of physical or mental aptitudes of human beings from artificial intelligence implements, will give rise to an era of the post-human species.

At this point, Vinge anticipates that the exponential development of artificial super-intelligence – which will no longer depend on inputs of human knowledge to continue creating – will have surpassed human intelligence and with it, possibly the ability to control, or even understanding, about the results generated by that[563].

How to forget, for example, the responses and reactions of the HAL 9000 computer, imagined by Arthur C. Clarke in "The Sentinel", and taken to the cinema by Stanley Kubrick in his masterpiece "2001: Space Odyssey"?

In the Space Odyssey, the artificial intelligence of HAL 9000 – in the on-board computer function of the spacecraft "Discovery" – is confronted with the decisions of the crew David Bowman and Frank Poole, who eventually plan to disconnect it. HAL 9000 discovers the plan, and considering Bowman and Poole as failed intelligences, continues to operate with the secret intention of annihilating them to ensure its own existence.

562 See Vinge (1993: 11).

563 See for example the incident of Amazon's assistant, Alexa, laughing out loud before her users without any apparent stimulus in <https://www.buzzfeed.com/venessawong/amazon-alexa-devices-are-laughing-creepy?utm_term=.dajoVqZYD#.fvmYXbOpV>.

28.2 From science fiction to reality[564]

The ability of HAL 9000 to act even with ulterior motives, contrasts with the hypothetical "laws of robotics" that Issac Asimov elaborated in the forties, in his story "Runaround" – later included in his famous compilation of stories "I, Robot "- just a few years before Alan Turing, in developing the test that bears his name (to determine the" intelligence "of a computer), incidentally created the term artificial intelligence as we use it now.

In "Runaround", Asimov proposes a set of rules applicable to alleged intelligent robots, which in essence orders them not to do or allow harm to human beings by action or omission; as well as obeying orders from human beings and protecting their own existence, unless such orders or the protection of their own existence come into conflict with the first approach.

Asimov's accounts challenge the apparent simplicity of these provisions, because once exposed to "real" situations, they create paradoxes, give rise to moral conflicts and ultimately serve as a pretext for Asimov to present – or anticipate, perhaps – the complex scenario of the relationship between human beings and machines that enjoy at some point a similar level of intelligence.

Although in our days the coexistence with a machine of behavior identical or substantially similar to that of a human being still seems far away, here is already the scenario in which an artificial intelligence mechanism is able to create another one, with better performance than the programmed one, originally by the human mind[565].

In appearance, that is the way to reach the technological singularity of which Vinge speaks: paradoxically, it will not be the human brain – with all its greatness and also with the limitations that by nature or for any other cause it may have – responsible for developing its intellectual pair; but it will be developed, in turn, by artificial intelligence.

This computational capacity requires a certain replication of the mental process, which is one of the reasons why this paradigm of artificial intelligence is usually associated with the concepts

564 See Iracelay (2017).

565 See Metz (2017).

of "neural networks". *(neural networks),* "Deep learning" (*deep learning*), or similar aspects; which imply, in essence, the ability of artificial intelligence systems to infer a result from data that is not necessarily exhaustive[566].

Let's put it this way: an artificial intelligence mechanism of this kind recognizes a prostrate kite, even if we have described it as a flying artifact; or distinguishes a dog even if we have not provided information on all the characteristics, images or perspectives of each and every possible dog breed.

The apprenticeship of human-in-human pain is authentically a "black box", in which we do not know for sure the shedding of interactions that occur to produce a response from certain information; similarly, artificial intelligence mechanisms that have transcended the mere notion of *"Machine learning"* – towards an *"Auto machine learning"*- they operate a similar function, through which it is possible to produce a result that does not necessarily depend on a foreseeable and invariable exercise, but has the capacity to consider new information or the same information under different circumstances.

In this context, it is easy to understand the reason why the "black box" of artificial intelligence, in its present tendency, turns out to be so fascinating and at the same time so disturbing: there are those who maintain that as soon as it is not possible to know or predict the chain of "reasoning" of an artificial intelligence system

- That is, that we cannot know what it "thinks", or how it reaches a certain action or response – we will have lost control over it and with it, the ability to take advantage of it.

The possibility of losing control over the development and effects of super artificial intelligence is essentially what some identify as a threat to humanity. Some futurists like Bill Gates, Stephen Hawking, Gerd Leonhard and of course Vinge himself, warn the latent risk of that circumstance[567].

---

566 See Wolchover (2017).

567 Some statements by Gates and Hawking can be read in*:* Rawlinson (2015) and Cellan-Jones (2014). As for Leonhard, his approaches are mostly concentrated in his book *"Technology vs. Humanity: The Coming Clash Between Man and Machine"*.

Elon Musk – CEO of Tesla and SpaceX, among other companies – shares this vision, and argues that artificial intelligence "is the greatest existential threat" for human beings. – *"With artificial intelligence, we are summoning the devil. It's like those stories where the character with the anagram and holy water is, and he's sure he can control it. And it turns out that it is not like that. "*- Musk said[568].

The vision of Musk brings to my mind a story published by William Bryk in *Harvard Science Review*[569], which in turn makes use of the basis of one of Fredric Brown's stories in *"Angels and Spaceships*[570]*"*: In the imaginary year of 2045, a group of Silicon Valley software developers successfully complete a program that simulates the human neural network in a computer interface. Before leaving to celebrate its magnificent achievement, the proud friends grant the new network full access to the Internet, so that it acquires information and is useful for executing tasks that they assign later. When returning from the celebration, the screen shows a strange message: "Program completed". The developers ask: "What is it that you have completed? To which the computer responds:" I know everything. Ask what you want. After deliberating carefully, the question they should ask, friends ask: "Does God exist?" The answer was: "It exists now".

Returning to Musk, it is interesting that in an unprecedented way – usually the regulatory proposals come from regulatory bodies, and not from the industry itself, he himself is one of the most vocal voices that calls for the regulation of artificial intelligence[571], along with other important players in the industry, such as Microsoft President Brad Smith[572].

With a different vision, Ray Kurzveil – together with Vinge, another of the most frequently cited authors in the field, particularly on the occasion of his famous work "*The Age of Spiritual Machines: When Computers Exceed Human Intelligence*"- is not particularly

568 See Gibbs (2014).

569 See Bryk (2015).

570 Specifically, the story of *"Answer"*, which is part of the compilation *"Angels and Spaceships"* by Fredric Brown, published by EP Dutton in 1954.

571 See Gibbs (2017).

572 See Bass (2015).

concerned with regulation as an element to which it recognizes a determining role in the transition from artificial intelligence to technological singularity.

28.3 How to regulate the black box of artificial intelligence?

What, then, is the role that regulation must assume around artificial intelligence? This is undoubtedly a very big and ambitious question for a short essay. However, I will enunciate five major considerations that in my opinion, should be taken into account in any eventual regulatory framework in this regard.

First, I have the impression that there may be an error of concept, on the occasions when it is proposed to "regulate artificial intelligence", as if it were a recognizable individual who can be allowed or prohibited conduct, and punished for a breach. In fact, although semantically lawyers themselves usually refer to the regulation of a subject, legal rules are concerned only with human behavior, unless of course it is an illegal or regulated activity, such as medical research with stem cells, in any case conducted by human beings.

In that sense, we can discuss the application or scope of existing rules applied to human behavior in relation to artificial intelligence, or even new standards if they are inapplicable or do not exist that should be applied; but in principle, to develop domestic legal frameworks, specifically aimed at artificial intelligence, in an attempt to foresee the different assumptions that this could create, would seem to me an absurdity at least at this moment.

For example, let's open our imagination and travel in time. Let's go back to the invention of telephone communications, and think of the amazement, challenges and opportunities that this incredible technological change produced in its time. Perhaps others, like us now, discussed the rules that had to be erected so that this invention was not used in harmful ways.

What would happen now if two individuals planned a fraud, or a murder, by telephone? Should we then, regulate the telephone to prevent this assumption?

In essence, the fraud or the murder continued to be the same human behaviors, whose nature did not change due to the fact that their commission implied, at some point, the use of a telephone communication.

Of course the example may seem crude now. I do not deny that it is possible that in time, the development of artificial intelligence forces us to rethink the whole way in which our laws are created, applied or interpreted in different legal systems – particularly, assuming that behaviors cannot occur executed by humans; but I argue that a priori domestic legislation, in a relatively nascent phenomenon, which would not yet be able to clearly identify legal assumptions substantially different from those already provided for in common legislation, would run the risk of preventing or making very costly the development of artificial intelligence in the country in question, which would operate against the essential purpose: that artificial intelligence serves to produce welfare to society. We are the first generation where Artificial Intelligence plays a preponderant role in our lives, and therefore the laws, regulations and current standards were not written in some cases to respond to it.

Second, I believe that the area of greatest regulatory urgency is located in International Law, to prevent mechanisms or weapons of artificial intelligence from being constituted as valid military instruments. For this example, it is necessary to build international consensus – That does not exist yet – so that weapons of autonomous behavior, drones or other extermination machines, are recognized as prohibited weapons.

In the same sense, an international agreement on cybersecurity and cyber defense is desirable. Both topics have high potential to take advantage of artificial intelligence mechanisms as part of their operation.

This type of agreement has been referred, for example, by the President of Microsoft, Brad Smith, as a proposal of "Digital Convention of Geneva" – not because it should be held in Geneva, but in reference to the Convention that was held in that city at the end of the Second World War, to create protective provisions in favor of civilians in times of war – to create what they should be

now, according to Smith, provisions applicable to the digital world in time of peace, or war[573].

It also falls within the scope of international law, the convenience of any regulatory framework on the subject, in essence global, based on internationally agreed foundations, facilitating regulatory harmonization and international procedural cooperation.

Not in vain recently Vladimir Putin, the president of Russia, said that *"Artificial intelligence is the future, not only for Russia, but for all humanity … It is accompanied by colossal opportunities, but also by threats that are difficult to predict. Whoever becomes the leader in this field will rule the world*[574]*"*. In this regard, China recently announced a robust investment of several tens of billions of USD in the development of Artificial Intelligence and its ambition to be the global leader in that field.

This single phrase of Putin, which illustrates without a doubt the importance that artificial intelligence has assumed in the global concert, demonstrates the need and convenience of an international agreement on the use of artificial intelligence technology for military purposes, cybersecurity and cyber defense, as well as minimum regulatory parameters that can eventually guide domestic legislations.

The third consideration has to do with two primary regulatory aspects, which by themselves are not necessarily tied only to artificial intelligence, but are currently part of the regulated topics of the technological sector: transparency and privacy.

However, it is possible that both vary their current regulatory tendency towards more casuistic rules of transparency and probably laxer privacy rules, according to which – according to the thesis of David Brin in his award-winning essay *"The Transparent Society: Will Technology Make Us Choose Between Freedom and Privacy?* – the fundamental premise of privacy will not be the right to "not be seen" by others; but the right – of transparency – to "see" others[575].

573 See Tworek (2017).

574 See Vincent (2017).

575 See Gowder (1999).

This variant, which at first sight could seem a subtle, implies a substantive modification of the current regulatory trend of privacy rights, usually associated with notions of information, use and consent, which would eventually move towards transparency rights. Accordingly, we will know if there is an interaction with an artificial intelligence system, if there are mechanisms to prevent undue discrimination or prejudice on the part of said system, or the means to know the decision process adopted by an automated mechanism, for example. The fourth consideration is the impact that artificial intelligence will have in very diverse areas of law, but that will undoubtedly have a significant impact on civil liability and objective standards. Perhaps in this area one of the most challenging aspects is located in achieving an adequate balance between a solid legal framework that effectively protects users and consumers of artificial intelligence products and solutions, but at the same time promotes innovation and does not establish an extraordinary regime of responsibility that discourages technological development. In the subject of limitation of civil liability, one should analyze the existence of a certification system where the solutions that follow certain rules have advantages in limiting their liability. In the area of product safety, there are those who have suggested the participation of the general public or holders of a legitimate interest with their comments and concerns based on risks through the publication of the codes and specifications by the developers of Artificial Intelligence, something like a Wikipedia. At this point, care should be taken that such publications are not to the detriment of the innovative and entrepreneurial spirit and there is transparency about the underlying business model.

Finally, and responding to the concern to ensure that Artificial Intelligence does not deepen inequality in the world, it is argued that governments should regulate for small entrepreneurs and small and medium enterprises have access to these developments and can multiply their effects in the economy and society. It is very important, in addition to ensure the participation of women, and minorities, so that such developments are inclusive, and represent the plurality of interests, cultures, interests and perspectives.

A recent Microsoft publication, prefaced by Brad Smith and Harry Shum, highlights an interesting area that will also suffer changes due to the development of artificial intelligence, which is that of economic competition[576].

Specifically, the growing concentration of information in certain economic agents may already be a concern for free competition nowadays – in particular, in the case of proprietary databases or for those that are not reasonably substitutable by open databases.

In this section, the study highlights the responsibility of the legal framework of the countries, to regulate the situations in which a certain concentration of information could constitute a barrier to entry into the market for new developers or suppliers of products and services related to artificial intelligence.

And a fifth consideration – that at least in logical order, perhaps should be expressed as the first – is the attention of domestic legislation to the regulatory assumptions that point to most studies on artificial intelligence regulation prospective[577].

Naturally, the most important regulatory assumption is the definition of what should be understood by artificial intelligence – which explains the reason why I mention this consideration at the end, assuming that there is some previous parameter established by international consensus –; followed by standards for research and development *(ex ante challenges)*, and norms to attend cases and solve problems of implementation of artificial intelligence solutions *(ex post challenges)*.

There are other issues of a more ontological order, but that could become regulatory efforts, in the development and implementation of solutions and applications of Artificial Intelligence, such as the impact on the automation of tasks[578], the consequent loss and creation of new jobs; the distribution of wealth created by these machines or systems; the consolidation of discriminatory practices

576 See "The Future Computed," published by Microsoft in <https://news.microsoft.com/futurecomputed/>.

577 See eg Scherer & Mendelson (2016).

578 See OECD (2016).

or prejudices; the need to integrate gender equality in the principles of solution development; the rights of robots, and many others that we do not know today. That is why several technology companies have formed an Alliance to define certain principles and values in the design of Artificial Intelligence[579].

28.4 Conclusions

The interest in regulating Artificial Intelligence has increased in recent times in the international community of legislators and regulators. Both the United Nations and the OECD[580], ITU, the WEF and countries such as Japan, Korea and the European Commission[581] are some of them. Undoubtedly Artificial Intelligence as outlined in this article carries great social implications, however this interest to regulate is influenced in some cases by fear of the unknown or its negative social effects, and was born in an era convulsed by the growing waves of populism and abuses in the use of social networks in democratic processes[582]. In that sense, the writer Cathy O 'Neil considers Artificial Intelligence as a challenge to the equitable distribution of income[583].

In essence, the set of considerations that guide an eventual legal framework in the field of artificial intelligence, must comply not only with the general principles of good regulation (usually expressed under the binomial of clear and proportional regulation, and not over-regulation), as well as per norms that encourage innovation, under principles such as the following:

- All projects should be able to be developed without the need for large-scale resources – that is, resources that are not reasonably universally available – (principle of discretion);
- All projects should be developed through processes open to any interested party (dissemination principle);

579 See <https://www.partnershiponai.org/>.

580 See <http://www.oecd.org/going-digital/ai-intelligent-machines-smart-policies/>.

581 As for example by means of the General Regulation of Protection of Data or commonly called "GDPR": Parliament and Council of the European Union (2016). General Data Protection Regulation For more information see Goodman & Flaxman (2016).

582 See Iracelay (2018).

583 See O'Neil (2016).

- The projects or technologies used in them, should not have the purpose or effect of being opaque to the regulatory entities (opacity principle).

Anyway, I will not share with those who have not read Millenium the findings of Frans Balder. But for the moviegoers, I leave that memory of the game of chess that HAL 9000 plays with Frank Poole: once the machine beats the man, we can assume that we are in transit towards the technological singularity of Vinge, and maybe then, the lawyers should start preparing our pencils. Why not convert some of the Asimov rules mentioned earlier in this article into regulation.

28.5 References

Bass, D. (2018). Increase in gig-economy jobs means tech companies have to step up to protect workers, provide benefits. Bloomberg Technology. <https://www.bloomberg.com/news/articles/2018-01-18/microsoft-says-ai-advances-will-require-new-laws-regulations>.

Bryk, W. (2015). Artificial Superintelligence: The Coming Revolution. Harvard Science Review. <https://harvardsciencereview.com/2015/12/04/artificial-superintelligence-the-coming-revolution-2/>.

Cellan-Jones, R. (2014). Stephen Hawking warns artificial intelligence could end mankind. BBC. <http://www.bbc.com/news/technology-30290540>.

Gibbs, S. (2014). Elon Musk: artificial intelligence is our biggest existential threat. The Guardian. <https://www.theguardian.com/technology/2014/oct/27/elon-musk-artificial-intelligence-ai-biggest-existential-threat>.

Gibbs, S. (2017). Elon Musk: regulate AI to combat 'existential threat' before it's too late. The Guardian. <https://www.theguardian.com/technology/2017/jul/17/elon-musk-regulation-ai-combat-existential-threat-tesla-spacex-ceo>.

Iracelay, J. (2017). De la ciencia ficción a la realidad. Nexos. <https://www.nexos.com.mx/?p=31902>.

Iracelay, J. (2018). Las redes sociales como desafío democrático. Nexos. <https://www.nexos.com.mx/?p=36348>.

Metz, C. (2017). Building A.I. That Can Build A.I. The New York Times. <https://www.nytimes.com/2017/11/05/technology/machine-learning-artificial-intelligence-ai.html>.

O'Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. New York: Crown Publishers.

Rawlinson, K. (2015). Microsoft's Bill Gates insists AI is a threat. BBC. <http://www.bbc.com/news/31047780>.

Scherer, M., Mendelson, L. (2016). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. Harvard Journal of Law & Technology, Vol. 29, No. 2. <http://jolt.law.harvard.edu/articles/pdf/v29/29HarvJLTech353.pdf>.

Turing A.M. (2009) Computing Machinery and Intelligence.

Tworek, H. (2017). Microsoft is right: we need a digital geneva convention. Wired. <https://www.wired.com/2017/05/microsoft-right-need-digital-geneva-convention/>.

Vincent, J. (2017). Putin says the nation that leads in AI 'will be the ruler of the world'. The Verge. <https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world>.

Vinge, V. (1993). The Coming Technological Singularity: How to Survive in the Post-Human Era. NASA Conference Publication 10129 Vision-21 Interdisciplinary Science and Engineering in the Era of Cyberspace. <https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19940022855.pdf>.

Wolchover, N. (2017). New Theory Cracks Open the Black Box of Deep Neural Networks. Wired. <https://www.wired.com/story/new-theory-deep-learning/>.

29 Leveling the Playing Field: Legal Assistance to .CL domain Name Holders

Margarita Valdés Cortés and *Humberto Carrasco Blanc*

Abstract

The widespread use of the Internet and its resources has meant that users of domain names are faced with a problem that is often unknown to them, such as conflicts about domain names. In particular, natural persons ignorant of these issues, faced with a controversy, do not act or defend their rights, in the context – in the case of this article – of an arbitration by domain names, in the electronic system of dispute resolution for top level domains for Chile, .CL.

We seek in our legal system the way to create a support space at no cost to users, mostly natural persons, for the defense of their rights and at the same time, could be an instance of academic learning of electronic litigation in the on line system of .CL and thus, is that in NIC Chile we call the Law Schools, in their course of legal clinic, to face this new challenge and among them, the Catholic University of the North.

The experience described in this article shows, in general terms, the way in which users can defend their rights and interests and how the dynamics in the trials and the quality of the arbitration sentences have changed when the holder of a .CL is legally advised**,** and additionally the social benefit that reports to the Chilean Internet community, free legal defense for their disputes under .CL. In particular, the experience of the collaboration agreement between NIC Chile and the School of Law and Social Sciences (FCJ) of the UCN is reviewed.

29.1 Introduction

The extensive use of the Internet has given rise to some legal issues related to its operation that need to be solved, such as domain name registration related disputes. A dispute resolution system has been designed for different types of domain names. Therefore, an international system (UDRP, Uniform Dispute Resolution Policy)

for generic domains (gTLDs) has been defined and adopted by some country code domain name (ccTLD) managers.

.CL domain users, through their registration agreement, have expressed their consent to solve any dispute via the .CL Local Dispute Resolution System (LDRP), which is based on the rules of the Dispute Resolution[584] Policy and the Rules for Domain Name Registry Operation[585].

The goal of this article is to describe a new free support program for .CL domain name holders, both from the point of view of NIC Chile and the Legal Clinic of the Master Course at Universidad Católica del Norte. The specific goal is to explain the origin of the program, its technical and legal aspects, the causes of system imbalance, the remedies that have been implemented, and some results showing an encouraging future for this program for the benefit of the weaker part in the dispute, which is often the individual user.

Finally, it is worth mentioning that this document is not intended to be a scientific paper.

29.2 Context and Assessment

The registration of .CL domains is carried out through a fully online process, at www.nic.cl, where a user account (User and Password) is created by filling out some fields with the required information. Thus, a user can register domains with all the data provided, without having to fill out new forms. For the registration process to be complete, a fee must be paid depending on the number of years for which a .CL domain is registered. Once the process is finished, the domain is added to the CL database, published in the zone and is ready to be used, by hiring e-mail and hosting services.

Disputes over domain names emerge when a third party believes that a registration infringes their rights due to confusion or similarity with trademarks, names of persons or company projects, commercial or literary names, etc. Unlike the UDRP, where the arguments are basically trademark law related, the Chilean system

584 See <http://www.nic.cl/normativa/politica-RCAL.html>.

585 See <http://www.nic.cl/normativa/reglamentacion_funcionamiento_registro.cl.pdf>.

covers also other types of rights. The mechanism to challenge a domain name registration under .CL is carried out through a request for revocation by filling out the online form[586] and paying a fee, published on the NIC Chile website[587].

The revocation action has two instances: an early 30-day period instance as of the domain registration date, and a later stage beginning after said 30-day period. Once the filing fee has been paid, the dispute management system notifies the existence of a revocation process, and it starts an electronic file, giving each of the parties a user name and password, so that they can interact on the file until its final processing.

Statistically, of all the arbitration proceedings concluded, 66% of the awards are in favor of complainants[588]. When there is a dispute confronting natural and legal persons – the latter generally represented by a legal firm – there is an imbalanced situation being produced when defending a good faith domain name holder, who naturally looks and feels weaker in the arbitration proceeding due to the lack of legal advice on how to proceed during trial and in the defense of their rights.

NIC Chile as the .CL registry has always been interested in improving information and legal defense conditions for domain name holders when faced with a conflicting scenario in a domain name-related arbitration procedure, either in the case of natural or legal persons. That is why we thought it was convenient, without losing the registry neutrality in these disputes, to be able to offer holders the option of this benefit, the possibility of receiving free legal advice, and to that end, we enlisted the aid of legal clinics at law schools as strategic partners to improve conditions for the legal defense of .CL domain users.

This provides for students a unique form of learning, because they will have the opportunity of operating in the .CL online arbitration system, which is unique in the country, and additionally, the user will be accompanied in all the stages of this arbitration procedure governed by the Dispute Resolution Policy.

586 The form is available at <https://www.nic.cl/rcal/ingresoDominioRevocacion.do>.

587 See <https://www.nic.cl/dominios/tarifas.html>.

588 See <http://www.nic.cl/rcal/fallos.do>.

This task involves assigning academic value to this legal advisory task, so that students may find this new procedure attractive and are able acquire tools to represent their clients in this online arbitration system, which does not call for face-to-face traditional legal proceedings.

For this convergence to be achieved, NIC Chile informs the .CL domain holder, when a dispute emerges, that legal aid provided by the Legal Clinic is available and will provide a link for the holder to send its data and to be contacted for a face-to-face or remote interview. The clinic will thus decide, according to its own procedures, whether to accept the applicant to be represented

Once legal representation is accepted and formalized, the student will be able to work on the electronic file on behalf of his or her client during the whole procedure until a sentence is pronounced, and the Clinic must take into account other admissible actions such as the filing of claims or appeals to be heard before higher courts. If no remedies are lodged, the sentence is executed based on the information provided by. CL and according to it.

It is worth mentioning that, on average, an arbitration procedure takes 4 months and awards are published in NIC Chile website[589], generating statistical information based on arbitration results.

Finally, it is possible to draft a report on the student's performance in the trial because proceedings are recorded in the electronic file logbook.

29.3 The Role of the Legal Clinic in the Mater Course at Universidad Catolica Del Norte (UCN)

This Legal Clinic is the result of a collaboration agreement between NIC Chile and the School of Legal and Social Sciences (FCJ) at the UCN. It is important to explain that there are several legal clinics collaborating with NIC Chile, and which depend on Finis Terrae University and Universidad Católica de la Santísima Concepción. However, in this article we will discuss the experience of the Legal

589 See <http://www.nic.cl/rcal/fallos.do>.

Clinic in the Master Course (MG) at the UCN (mention in Business Law (DE)) and its particulars. Bear in mind, each clinic has its own processes to assist .CL domain name holders.

One particular aspect of the UCN Clinic is that it works with students from Antofagasta and Coquimbo, the venues of the school. Likewise, all legal clinics at UCN work with the Service Learning methodology (A + S)[590,591]. This legal clinic at the Master course uses the same methodology. Another feature is the existing interaction of undergraduate students taking the final year of their degree course with master course students, thus creating a sort of virtual legal firm.

The objectives of this clinic can be summarized as follows:

a. To provide students taking the Master course in Business Law at the School of Legal Sciences at UCN knowledge and experience in the filing of domain name- related proceedings.

b. To encourage teamwork among clinic undergraduate and master course students, both with mention in Business Law.

c. To interact between the clinics of the Antofagasta and Coquimbo campuses.

d. To contribute to the development of domain name- related legal dogmatics through articles, theses or portfolios produced by students taking the Master course.

The Clinic methodology can be classified into two lines of action:

a. Preventive advocacy: To address domain name holders´ questions in terms of revocation processes. This activity involves, among other things, answering questions from domain name holders, reviewing contracts or other alternative path to a domain name arbitration process.

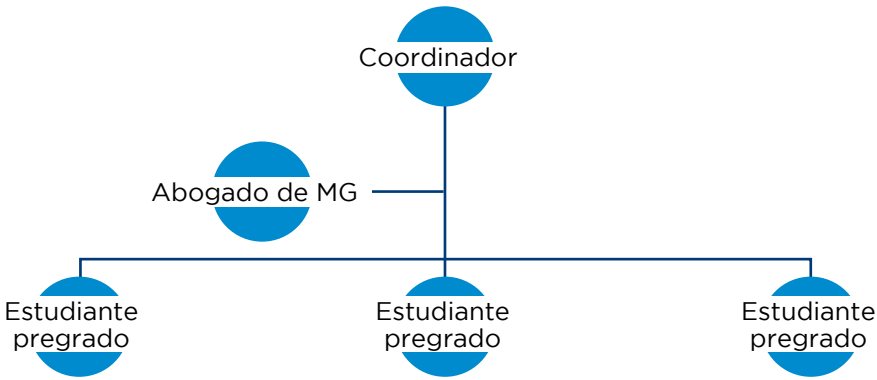
590 Puig Rovira has stated that "... service learning is a pedagogical methodology with a great educational power. A methodology combining, in one single activity, content learning, skills and values in order to accomplish community service tasks. In service learning, knowledge is used to improve one community aspect, and the service turns into a learning experience creating knowledge and values. Learning and service are linked by a virtuous circle where both parties get benefits: learning acquires a civic sense, and service becomes a workshop for values and knowledge". Casares et al., 2009, p. 9

591 Academics at UCN apply Learning + Service modality when training their students, <http://www.noticias.ucn.cl/destacado/academicos-de-la-ucn-aplican-la-modalidad-aprendizajeservicio-en-la-formacion-de-sus-alumnos/>.

Remedial advocacy: This is the legal defense of domain name holders in arbitration processes filed via a digital platform and resolved by arbitrators.

29.3.1 Structure and Fucntions of the Legal Clinic

The clinic structure is based on the following scheme:



Source: Legal Clinics Project NIC Chile-UCN, Open NIC 30 years, p.5

First, there is the coordinator who is in charge of overseeing the Legal Clinic and leading case defense strategies. Second, legal clinic students at the Master course are in charge of developing the arguments, and they participate in advocacy strategies and answer complaints. Finally, undergraduate students generally perform procurement tasks, i.e. requesting domain name holders' background information and documents, sending order forms, searching for case law, requesting changes in notification emails to the Dispute Resolution Center, and finally preparing the answer for the revocation request.

One relevant characteristic is the virtual nature of this interaction: the coordinator, the lawyer at the Master course, and undergraduate students communicate among themselves and with clients through electronic means. To this end, video conferences via Skype or Zoom.us are used. As an interesting precedent, only one domain name holder being represented is domiciled in Antofagasta. All the other clients are domiciled in different cities of Chile.

29.3.2 Legal Clinic Experience Results

The following table shows the internal statistics and the results as of the date of this article (1/16/2018):

Domain name consultation	Legal proceedings	Judgment in favor	Judgment against	Agree ments	Abandoned clients	Terminated by no payment	Pending
89	65	21	9	6	6	8	15

It is possible to conclude from legal proceedings and dispute resolution that 70% of the cases were resolved in favor of domain name holders. This shows a clear improvement of the imbalanced conditions existing before the implementation of legal clinics.

According to legal clinic students, the following benefits are created:

a. For undergraduate and graduate practitioners, this means exploring and gaining experience in legal areas they would not be able to access in the region.

b. For the master program, the clinic brings benefits from two perspectives:

- It is a new opportunity for obtaining a degree with mention in Business.
- It provides legal knowledge on specific Internet-related issues.

This is due to the articles and portfolios produced by this clinic, which are defended before a panel of experts at the master course.

29.4 Conclusions

Both from the point of view of NIC Chile, as well as the Legal Clinic of the Master Course at Universidad Catolica del Norte, the legal aid program for domain holders has brought benefits to several stakeholders, as stated before. In summary, this has become a virtuous circle contributing to bridging the existing gap between

complainant and domain name holders subject to an arbitration process, and therefore, leveling the field.

29.5 References

Dispute resolution policy <https://www.nic.cl/normativa/politica-RCAL.html>.

Rules governing .CL domain name registry operation: <https://www.nic.cl/normativa/reglamentacion.html>.

Dispute resolution allocation statistics per .CL domain names: <http://www.nic.cl/rcal/fallos.do>.

Uniform Dispute Resolution Policy: <https://www.icann.org/resources/pages/udrp-2012-02-25-es>.

Academics at UCN apply the Learning + Service modality in the training of their students, "UCN News to date – Universidad Católica del Norte. (s. f.). Recovered February 19, 2018, from <http://www.noticias.ucn.cl/destacado/academicos-de-la-ucn-aplican-la-modalidad-aprendizajeservicio-en-la-formacion-de-sus-alumnos/>.

Casares, M. G., Toledo, M. D. la C., García, X. M., Martín, M. G., Rodríguez, J. P., Rovira, J. M. P., Castelló, M. T. C. (2009). *Aprendizaje servicio (ApS): Educación y compromiso cívico.* Grao. <https://www.nic.cl/normativa/reglamentacion.html>.

30 E-commerce in Mexico

Julio César Vega Gomez

Abstract

The adoption of the Internet during the last 20 years in Mexico is a reality that today is especially tangible through online transactions. Electronic commerce has evolved by leaps and bounds and more and more companies from different industries, including traditional ones, see online commerce as a sales channel option. Companies of all sizes have started their way in the adoption of electronic commerce, and consumer confidence, although it still has areas of opportunity, is favorable to electronic transactions and the market invites companies from different countries every day to join the Mexican market.

Notwithstanding the foregoing, today the threats come from the regulatory trench, where there are more and more attempts to regulate the Internet and in the particular regulate electronic commerce and not with an equitable vision between consumer protection and the development of companies; rather, and in many cases, there is an unclear vision of the functioning of this innovative sales channel and the particularities of it. This happens at the time that adequate public policies have not been issued to have an even more powerful ecosystem and avoid a possible commercial digital divide. Thus these are the realities and challenges of one of the main economies of Latin America.

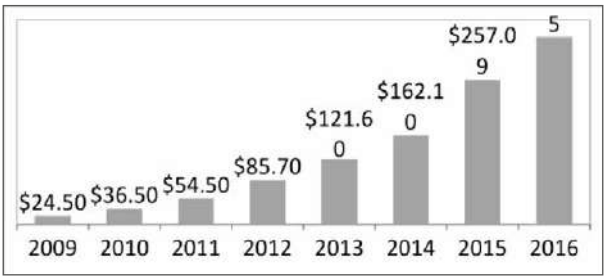
30.1 Introduction

The evolution of this commercial phenomenon has occurred since the end of the nineties in Mexico, which is not alien to the commercial dynamics in this line of its northern neighbor, and main commercial partner. Notwithstanding the above, and as in other markets around the world, during the so-called "dot-com bubble"[592],

592 For an explanation of the "bubble dot com" thermos, see <https://es.wikipedia.org/wiki/Burbuja_dot com>.

period of heightened speculation by nascent companies based on the Internet, there were various problems and many companies went bankrupt, were acquired by larger companies or better design for the digital era or, in a few cases, survived the debacle.

In 2013, Mexican entrepreneurs continued the adoption of e-commerce practices. Already in 2011 the figure of 45 billion pesos of goods sold through electronic commerce was exceeded and for 2012 it maintained a growth rate of 45% per year, according to the research carried out by the then Mexican Internet Association (AMIPCI), today Internet Association.MX[593]. Today, in 2017, with figures referring to the last year, Mexican e-commerce has reached the figure of 329.85 billion pesos[594] in transactions, giving us a cumulative growth of 383.7% from 2012 to 2016:



* Figures in billions of Mexican pesos.

Source: Asociación Mexicana de Internet, AC Compiled of growth of electronic commerce in Mexico.

Year	Sales Value	Previous Year
2016	$329.85	28.3%
2015	$257.09	59%
2014	$162.10	34%
2013	$121.6	42%
2012	$85.7	57%
Variation 2012-2016		**383.7%**

This hopeful reality is due to the growing consumer confidence in the channel, having 3 of every 4 national Internet users already make some purchase online[595].

593 Internet Association.MX before AMIPCI: <https://www.asociaciondeinternet.mx/es/estudios>.

594 See Association of Internet.mx. (2017).

595 *Ibid.*

30.2 The catalysts of electronic commerce in Mexico

The travel sector continues to be the leader in this area with almost 30% of the total national figures, as shown by the studies of the Mexican Internet Association, and in regard to consumer goods, fashion items (footwear, clothing and jewelry) are the categories that lead the tastes of the Mexican consumer. There are many causes and here are the most important ones:

- Consumer Confidence
- Ease of making purchases online through smartphones (90% of buyers have at least one mobile device with these characteristics)[596].
- Accessibility of means of payment
- Greater offer on the part of the shops
- Offer of low-value digital goods (applications, music, video games etc.)
- Arrival of globally recognized competitors (Amazon arrived in 2015 and Alibaba plans on opening offices and consumer commerce operations in 2018, this 2017 presented credentials to President Peña).

As can be highlighted, none of the above reasons is a comprehensive public policy, that is, the catalyst for electronic commerce in Mexico has not been a deliberate public policy, however, some of the previous items are linked to reforms or programs of government that I will highlight later. According to the Report on relevant actions of the Ministry of Communications and Transport January 2013 – June 2017, some of the benefits generated with the implementation of the constitutional telecommunications reform[597] are:

1. In terms of coverage. – The reduction of the digital divide going from 41 million users to more than 65.5.
The previous statement does not find a basis in the figures[598] of InternetMX, the first institution that made a measurement in this

596 *Ibid.*

597 For an executive summary of telecommunications reform, see <https://www.gob.mx/cms/>.

598 See Studies of the habits of Internet users in Mexico <https://www.asociaciondeinternet.mx/es/studies>.

regard, and the only one that has done it uninterruptedly for 13 years. This increase in official figures responds to a change in methodology, and not to the effects of the reform. This case is similar to what happened with the measurement of poverty that was widely and deeply criticized by the National Council for the Evaluation of Social Development Policy (CONEVAL).

2. Reduction of prices in telecommunications. – 43% reduction in mobile telephony services.

The above, added to a growing number of open connection points or WiFi[599], has served as a trigger for the electronic commerce sector in terms of access. The problem in the process of resolution in the context of electronic commerce, is the demand. More connected people are more potential consumers and the figures indicate that with the passage of time and the perceptibility of the points that previously stood out, this possibility could materialize.

On the other hand, in terms of public policy and electronic commerce, we can highlight the Program for the development of the software and innovation industry PROSOFT[600], belonging to the Ministry of Economy, under the administration of the Under secretariat of Industry and Commerce and currently operated by the General Directorate of Innovation, Services and Domestic Trade[601]. This program was conceived in the administration of President Ernesto Zedillo Ponce de León, and launched in the administration of President Vicente Fox Quesada, continued by President Felipe de Jesús Calderón Hinojosa.

The aforementioned program finds its sustenance at the moment in the Sectoral Agenda for the development of the Information Technology in Mexico (2014-2024)[602]. This agenda is particularly relevant to the effect of this essay, with regard to the digital market and specifically, with regard to strengthening confidence in electronic commerce. This latest public policy

599 It is not advisable to carry out electronic commerce operations in open networks due to the danger of using financial data in the transaction and the possibility that these will be stolen in an open channel.

600 See <https://prosoft.economia.gob.mx/>.

601 See article 26 of the Internal Regulation of the Ministry of Economy, available in <http://www.diputados.gob.mx/LeyesBiblio/regla/n163.pdf>.

602 See <https://prosoft.economia.gob.mx/doc/Agenda%20sectorial%20PROSOFT%203.0.pdf>.

effort is aimed at solving the problem of supply in electronic commerce through the following areas:

- Conduct studies of the sector.
- Carry out promotional e-commerce events.
- Strengthening existing e-commerce platforms.
- Strengthening e-commerce software development.
- Opening of new electronic stores.
- Opening of electronic sales channels in traditional stores.

In both cases of public policy, both in the telecommunications reform aimed at improving demand and in the PROSOFT program aimed at increasing supply, we have seen positive results, although still insufficient. The role played by the State in this matter has been rather distant, more in accordance with the non-intervention proposed by Adam Smith; however, and from my point of view, the intervention should have been more like the proposal made by "The Mercantilists of the eighteenth century" because the State had to actively promote commercial and industrial development due to the sui generis situation of the development of information and communication technologies in the United States of North America, the main commercial partner of Mexico.

30.3 A critical view of the current situation

Today, in the Mexican jurisdiction, we experience more development in consumption than in the opening and expansion of companies linked to online commerce and in terms of technology -- few are the Mexican companies that provide platform services to traditional businesses. The Mexican market in this area has been distinguished by the adoption of options from foreign platforms, Mercado Libre or Amazon, although efforts are already being made with national capital, such as Linio or Osöm.

It is natural to think of the lack of information as the main failure of the State in terms of momentum, since the vast majority of technology and Internet-based business models came from other countries. In 2017, for example, the main player of the ecosystem, MercadoLibre,

celebrates 18 years of operations in Mexico, and at that same time the country does not yet count with a comprehensive public policy. Hence, I dare to state that the public policies mentioned earlier in this document have been neither efficient nor effective in meeting the needs of an increasingly sophisticated market that is constantly evolving both in terms of growth and complexity in its business aspects, as e-commerce through social networks or social commerce, or commerce in the Internet of things, trade between the consumer and robot or trade within the framework of artificial intelligence.

The main faults are:

- The lack of consumer confidence that, although it has decreased, still prevails. This barrier is commonly fueled by the government's own misinformation as the quarterly reports[603] of the National Commission for the Protection and Defense of Users of Financial Services (CONDUSEF).
- A historical friction between merchants and banks in terms of chargeback, which among other things, has resulted in an imperfection in the chain, to take an unnecessary step offline, since consumers prefer to make payments in person at stores of convenience or pharmacies.
- The disproportionate prices in parcel and courier services.
- Lack of regulations that encourage and do not restrict online commerce.
- Lack of specialized human capital.
- Support to the micro, small and medium-sized company segments.

30.3.1 Other latitudes

Regarding how the problem has been solved in other places, it is important to highlight that, in the countries with the most vigorous electronic commerce, this phenomenon was never seen as a problem and instead as an opportunity. The United States, but

603 See <http://www.condusef.gob.mx/gbmx/?p=tipos-de-fraude>.

mainly the United Kingdom[604], have been able to capitalize in an extraordinary way. The threats mainly in Europe come from the regulatory field where associations and foundations make efforts of coordination and lobbying to avoid regulation that hinders the dynamics of trade.

A separate case is of the opportunities in developing countries where small and medium enterprises are the majority and the engine of the economy. For such purposes, the World Trade Organization issued a few months ago some thoughts that I think are important to consider in this essay[605].

These include the selection of the best sales channel depending on the business model of this segment of the company in which the own pages are included, the *market places* or electronic commerce through social networks. The challenge of obtaining qualified human capital for the operation of online commerce is also noteworthy.

30.3.2 Steps to follow in Latin America and the Caribbean

To analyze our region in general terms, it seems prudent to take a step back and review our inclusion in the international digital ecosystem. According to the report of the Economic Commission for Latin America (ECLAC) 2016, the region reports that in 2015, the 55% of its population connected to the Internet[606], an encouraging figure but far from the average of the countries of the Organization for Economic Cooperation and Development (OECD) that reports[607] 85.34% of people connected. The aforementioned poses an access problem that necessarily, and even in the case of being solved, will later pose the challenges inherent to the adoption and use of the Internet.

---

604 According to data from the eCommerce Foundation, plate 33, the United Kingdom has the highest participation rate of electronic commerce in the Gross Domestic Product. See <https://www.ecommercewiki.org/Prot:Ecommerce_Europe_European_B2C_Ecommerce_Country_Report_2017_%28free% 29>.

605 These reflections can be consulted integrally in <https://www.wto.org/english/res_e/ booksp_e /ecom_brochure_e.pdf>.

606 ECLAC (2016).

607 See OECD (2017),

We must be aware that in the region we must reduce the different adoption gaps such as access, gender, generation, connection quality etc. This step back in terms of access, adoption and use must coexist with the evolution of the Latin American digital economy and specifically with regard to online commerce which, as I have already stated, at least in Mexico, grows double-digitly each year.

It is imperative that the current and future benefits of electronic commerce reach all segments and sectors of national economies with a spirit of global competition, aspiring to achieve the most advanced international standards.

30.4 Conclusions, reflections and suggestions

I consider it of vital importance that there is genuine coordination between the different actors of the public sector in order to be able to articulate an integral policy of electronic commerce in Mexico that is feasible while being compatible with the most successful international models in the world. Due to the current barriers, my intervention suggestions from the relevant actors are the following:

- Ministry of Economy: before any interagency effort, it is necessary for this dependence on the federal public administration to define a sector strategy to be able to carry out an effective coordination between the different administrative units within it.
- The National Institute of the Entrepreneur deserves special distinction, which should boost the growth of the associated SMEs to electronic commerce to achieve equity with the great platforms that flourish in Mexico.
- National Banking and Securities Commission: in coordination with the previous agency and the private sector, it must propose solutions to distrust in the banking system and the increasing use of cash in electronic commerce.
- Postal Service in Mexico: needs to modernize to be able to compete with the large parcel and courier companies and become a real option that can lower costs.
- Ministry of Public Education: should create a map of technical and professional careers involved in electronic commerce and

promote a modernization of the curriculum in the resulting careers, so that graduates have the necessary knowledge to enter the labor market with well-paid jobs.

For all of the above, the efficiency of the resources invested must always be sought with the goals that are sought in each case. It is necessary to review the internal regulations of each unit to fully incorporate this activity and channel more resources and even eliminate some activities that today, thanks to the use of technology, are obsolete.

30.5 References

Asociación de Internet.mx. (2017). Estudio de Comercio Electronico en Mexico 2017. <https://www.asociaciondeinternet.mx/es/component/remository/func-startdown/72/lang,es-es/?Itemid>.

Comisión Económica para América Latina y el Caribe (CEPAL) (2016). Estado de la banda ancha en América Latina y el Caribe 2016. <https://repositorio.cepal.org/bitstream/handle/11362/40528/S1601049_es.pdf?sequence=6&isAllowed=y>.

Organización de Cooperación y Desarrollo Económico (OCDE) (2017). Digital Economy Outlook 2017. <https://read.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-outlook-2017_9789264276284-en#page34>.

31 A Connected Synthesized Existence: how the Internet Could Enable 3D Printing to Improve the Developing World

Mark W. Datysgeld

Abstract

While transformative technologies such as Artificial Intelligence have attracted a lot of attention from academia and the media over the years, the subtler development of additive manufacturing has not yet been recognized as an important factor in shaping our future. In this chapter, we try to understand how the combination of a constantly expanding Internet with the increased availability of 3D printers will provide opportunities for improvement for the developing world. After reflecting on the paradox of globalization that leads to raw materials being sent around the world only to be returned as finished products, we proceed to make our analysis based on empirical research and technology that is already beyond the testing stage of the concept, looking at examples from the sectors of construction, health and food. With this data in hand, our research moves towards understanding the intersection between the consequences of 3D printing on a larger scale, a global communications network and intellectual property rights. We outline some possible policy routes to turn these developments into benefits for the developing world, while taking into consideration issues such as job relocation. Our conclusion is that before the world is taken by surprise by the manufacture of additives and policies are promulgated in a reactive manner, it is the responsibility of the actors involved in the relevant arenas to advance a meaningful discussion on the subject, while there is still time for the creation of a more sustainable logic for our productive system.

31.1 Introduction

When discussing the Internet and its policy-making processes, it is often more practical to emphasize procedures that are immediately relevant to the network and its functions, often forgetting the

cross-cutting role it plays over multiple emerging areas that are still taking shape. The development of most technologies now depends on how the network works, since it has become the default bridge that connects the different social actors that generate technical progress from the campuses, industries and Households around the world.

In this sense, when considering the developments in production and the direction that economic models will take in the near future, it is key to observe how the Internet is being formed, since it is the de facto international pillar of intellectual property rights, commericial relationships, generation and distribution news, along with several other factors that inform how technologies are developed and what expectations they must meet.

In his book "War in the era of intelligent machines", Manuel DeLanda (1991) reflects on the fact that once, when clockwork mechanisms were the predominant vectors of technology throughout the world, people tended to imagine the world that surrounded them as a system of gears and wheels. A person who was important for an operation but easily replaceable was just "a gear in the machine" or a "gear in the wheel". To facilitate a situation was "grease the wheels".

The Internet occupies a similar space in our collective understanding of the contemporary world, at least as far as the majority of the people in the connected half are concerned. To "send messages", someone wants to reach them instantly through the Internet; we have come to think of our friends as real people and as abstractions on a screen; "We evaluate" that is being viewed in real time from around the world with a single click and "close" with the same ease. In this sense, when the paradigms are reconsidered, the Internet cannot be eliminated from the equation, but must be one of our central concerns.

Of the many oddities of the contemporary world that do not seem to be aligned with our digital existence, there is the state of the industrial process. Creating a part of something, whether machinery or not, depends on a production chain that begins with the raw materials that are extracted from the soil, then homogenized and sold as merchandise, sent to a factory that is often transferred to the

factory desired part, then sent to the final consumer, which could be from the same country from which the raw material was extracted.

A quick look at the trade relationship between Brazil and Japan illustrates a scenario that is consistent across the developing world[608], once we observe that the main export from Brazil to Japan is iron ore, while its main import are pieces of cars and tractors (Itamaraty, 2016). Is it efficient to send rough iron half way around the world only to be shaped into pieces and then imported back into the country in which the extraction was made?

31.2 The paradox of globalization

As the process of globalization intensified and communication technologies became more advanced, this system prevailed despite its inherent lack of sustainability. As a process, it works to the extent that we consider that, at the end of the day, the products are delivered to customers, despite the long and strange journey that these products must undergo. However, it should not make sense to ship a product through this process and still end up with a lower cost than if it were manufactured in the country from which the raw material was extracted.

The answer to that question is well known at the moment, but it is still widely ignored for convenience: the exploitation of people living below the poverty line is the driving force behind this model. China can be seen as an example. Despite being the world leader in exports (CIA,2016), the country still has 40% of its population living on less than $ 6 a day, and its huge rural population continues to be relocated throughout the country in accordance with government strategies aimed at keeping constant the expansion of its industrial power, although these workers may end up unemployed and marginalized when production plans do not materialize (Chow, 2018).

Conceptually, the development and distribution of quality products sold at more affordable prices through a connected global network should tend to generate better results, increase

608 Whenever we refer to "the developing world" in this chapter, there will be a focus on Latin America, since it is the region that best fits the scope of this research. However, given the similar nature of the struggles in the periphery, it can be assumed, in general terms, that the questions posed here find equivalences throughout the developing world.

global access to technology and help balance opportunities in the workforce. The problem then lies in the way companies associate with governments to exploit their combined strength in order to generate as much surplus as possible without taking sustainability into account, modifying even the best aspects of capitalism into something harmful. Worse still, at a higher level, these same corporations and governments fight with each other for taxes and the right to evade or retain them (Shaxson, 2011).

All this has become a key part of the common perception of how contemporary production and trade work, which, in addition to very specific issues, such as the homemade manufacture of plastic guns, has gone unnoticed by the general population. The revolutionary process of additive manufacturing has become faster, more portable and much cheaper than it used to be. The idea that in the near future we can avoid more and more of this industrial process has not yet reached the perception of the majority.

31.3 Additive manufacturing arrives

Better known as 3D printing, the additive manufacturing process has a number of advantages and disadvantages over traditional subtractive manufacturing. As time passes, an international community of creators is forming, sharing three-dimensional models in operation and improving them collectively, while offering support to newcomers in a multitude of languages through the Internet. The leading website Thingiverse has built up a database of more than one million objects from 2018 onwards, and has a thriving community organized around different interests related to the manufacture of additives (MakerBot Thingiverse, 2018).

An area in which the manufacture of additives is far superior to other methods is in terms of reducing the waste of materials. By imitating the way in which the natural world is assembled, drop by drop, only the raw material that will be used in the final design is heated and converted, for example, from plastic filament into a real piece. That piece is assembled layer by layer, with the density and the desired characteristics, without leaving material to be discarded. Even so, the recycling of excess material is easy and can be done economically (Harding, 2016).

Notable disadvantages lie in the fact that devotees of technology consider the process "messy, sandy, and difficult" (Rundle, 2014). It cannot be ignored that the process consists essentially in melting or breaking raw materials to condense them in a different way, a process that would normally occur within industrial complexes far from people's daily lives. Transferring this procedure to social spaces means that solutions must be found to accommodate them better. The difficulty of the process is also relative, often not to the impression itself, but rather in relation to the design of the model and the finishing of the piece, which may require some engineering knowledge, as well as the chemical and physical effort.

This technology has come a long way in a short time. Born in the 1980s with the purpose of making rapid prototypes for the industrial sector, it only began to take its toll on the domestic market in 2005, when mechanical engineer Adrian Bowyer began to publish in open code the plans of his blog for RepRap, a 3D printer that could print copies of itself, needing only to be assembled with an engine ready to use to function (Rundle, 2014). With this opportunity, developers from around the world began to experiment with the manufacture of additives, which eventually led to the creation of MakerBot, the most popular printer on the market, reaching 100 thousand machines sold in 2016 and retail sales around of 2,500 US dollars. (Watkin, 2016).

The flexibility of the additive manufacturing process is impressive, not only when considered as a way to produce finished goods without the need for intricate artisanal or industrial techniques, but particularly because of the potential to adopt this efficient production approach to demand in countries that have not fully reaped the benefits of the industrial revolution, and still depend on other actors to finish the products they consume.

When we consider the struggles of the developing world, many of the problems faced by countries such as those in Latin America fall within the scope of basic, innovative solutions that are necessary to navigate them. For example, the region has greatly exceeded the late arrival of the Internet by jumping directly from personal computers to access via mobile phones, and at the moment it is the second fastest growing mobile market in the world (GSMA, 2016).

This shows how it could be more valuable for the developing world to seek its own solutions instead of following the path already traveled by developed countries.

In this sense, we will now give a brief look at three fields in which the transformation potential is already demonstrable outside the realm of science fiction, with tangible solutions that could soon begin to be implemented so that the developing world looks for innovative solutions and achieves the proposed goal of finding answers that deviate from the formulas that are already in use.

3D printing was once limited to smaller objects, but this has changed drastically, and the printing of entire houses and structures has been proven by companies around the world since 2014. Using some form of concrete powder or even waste like ink, these houses are cheap, quick to build and produce reliable final results. The tallest building printed so far is 16 meters high, and a Chinese company has managed to produce 10 houses in a single day, demonstrating the scalability of the technology (Koslow, 2017).

In the developing world, this type of solution could be used to achieve an affordable mass production of housing, as well as to provide a rapid relocation of living spaces after natural disasters, which remains a major concern. Between 1990 and 2011, researchers found that the minimum losses in the housing sector for 16 countries in Latin America and the Caribbean amounted to $ 53 billion, and reconstruction efforts were often not enough to produce decent results (Nations United, 2013).

Another field in which 3D printing is rapidly emerging is health. With regard to prostheses and implants, the use of this technology allows patients to receive mechanical parts of the body that adapt to them from the beginning, helping to adapt and comfort. This has been a struggle throughout the history of prosthetic development, since human beings have the potential to reject foreign bodies due to physical and psychological concerns, in such a way that advances to make this process smoother and more they have always been key (Ventola, 2014).

Preliminary tests of printing with live tissue as ink are being carried out, with the aim of producing replacement organs in the future,

but the printing of small-scale body parts is already becoming a certainty. Cornell researchers have used the additive manufacturing process to print human ears with gels made from living cells such as ink, and in three months those structures are converted into flexible ears with cartilage that can be used as almost identical replacements (Cornell University, 2013).

Once again, the struggles of the developing world in the health sector are persistent, broad and systemic and are affected by layers of corruption, mismanagement and simple inefficiency. Innovative solutions, such as those summarized above, are ways to begin to replace costly imports to provide cheaper and faster support to the sick and homeless.

Finally, the production of food is a subject that still exists outside the manufacture of additives, since only recently viable options began to emerge in this sector. While hunger is being eradicated slowly throughout the world thanks to advances in technology and logistics (United Nations, 2014), the fact that a person has something to eat does not necessarily mean that their diet is ideal for their development or that this allows them to lead a healthy life.

With the ability to refine food, it would be possible to create nutrition that is rich in the necessary vitamins and with the target caloric quantities, as well as guaranteeing its greater durability and the ability to better plan the distribution, creating more efficient public policies frames that bring food to regions that would normally be affected by distribution and management problems. Currently, printed groceries are only offered as novelties in high-end restaurants, but there is no reason for the situation to continue like this (Wiggers, 2017).

31.4 The Internet of printers

The umbrella that unifies all these solutions and many other possible ones is the Internet. Different 3D printers are required to perform different tasks, in such a way that it makes more sense to centralize and serve a community instead of individualizing. These could be combined as a combination of state, privatized and multi-source initiatives, but the key result is that with the help

of connected devices, families could interact with these printing services according to their needs. Together with the collection of aggregate statistics, this would allow a more detailed analysis of the needs of each region, helping to formulate better policies.

However, there is a complex and barely discussed set of questions that must be examined before these potential benefits can come true. In the past, revolutionary technologies in general have been met with skepticism during their childhood, until they are proven to be viable, and by then preventive measures can no longer be taken. While creations that look impressive like robots and artificial intelligence have entire university departments devoted to studying the philosophy and economics of their implementation, the subtler 3D printing technology remains largely ignored, emerging in the background (Rundle, 2014).

This chapter will now attempt to analyze in a non-exhaustive way two key aspects that will make or break the adoption of additive manufacturing as one of the solutions to problems in the developing world: first, in the case of large-scale adoption 3D printing is possible thanks to the formulation of policies driven by innovation, how the current productive environment will be affected by these changes and, secondly, who will be the owners of the plans and how to apply the laws of intellectual property under this new productive reality? For the first point, if history serves as a guide, the answer is that such transitions are often complex and tend to cause instability from the start. This is due to the fact that changes brought about by a paradigm shift make it impossible to maintain the status quo, and although some activities and business models can catch up, many others simply find it impossible to do so. While some actors work to reinvent themselves, others try to stifle progress and seek regulatory or other measures to prevent the rapid adoption of the new technology.

The widespread adoption of the telegraphic system in the late nineteenth century forced drastic changes in commerce, journalism, human relations, crime and war. The same can be said about the Internet, which greatly magnified the effects of the telegraphic revolution. The consequences for trade in particular were significant, leaving a deep mark on companies around the

world, and although previously prices had to be formulated with a combination of historical data, attention to trends and a good deal of guesswork, all of a sudden it was possible to communicate the shortages and surpluses in a matter of minutes. This made the markets have to react much faster and become more malleable, making use of other technologies, such as tracking weather patterns, and reacting to the ever changing results. Needless to say, the Internet has taken this to a completely different level, with investors struggling for fractions of seconds to obtain information that will provide them with an advantage (Standage, 2014).

In assessing the current state of the market, the process described above of raw materials traveling around the world before returning as finished products could be significantly reduced. While high-end circuits would still have to be imported from developed countries, plans for simpler objects could be circulated and produced locally, including spare parts for local industrial machinery, and move towards the adoption of more complex techniques to produce more specialized pieces. On-demand production based on recyclable materials would also mean less waste and firmer control of sustainability, which in turn would help combat the accumulation of waste and, as a result, reduce the risk of flooding and the spread of diseases. This would generate gains for sustainability without requiring additional effort, but in an optimistic scenario in which there is a proactive participation of the government, the maintenance of the products could be more constant and a culture of repair and reuse could be encouraged, which makes sense when the per capita profit is not high (Ford and Despeisse, 2016).

Several products that are currently branded or that depend on specific manufacturers could be produced locally by independent third parties, including wheelchairs, auto parts, projectiles for electronic devices and even more complex multi-part devices. For populations with limited expenses, this could allow the maintenance of a higher standard of living by paying less for the same products; many of which currently reach abusive prices in the developing world due to import taxes and varied clandestine treatment. All this has become a key part of the common perception of how contemporary production and trade work, which, in addition to

very specific issues, such as the homemade manufacture of plastic guns, the potential has gone unnoticed.

The revolutionary process of manufacturing additives has become faster, more portable and much cheaper than it used to be. The idea that in the near future we can avoid more and more of this industrial process has not yet reached the perception of the majority. As far as China is concerned, the productive giant seems to be one step ahead in the game, and many of the additive manufacturing strategies described in this chapter are being led or supported by Chinese companies.

The country may begin to lose profits due to the export of certain goods, but the higher income from its exports comes from machinery in recent years, despite the high volume of imports of integrated circuits (WTO, 2016). As the country begins a slow march of impoverishment, other Asian markets also begin to look more attractive to corporations for their low wages, so the jump from China to the next step of the industrial revolution is logical. For the second point who will be the owners of the plans and how the application of intellectual property laws will be carried out, again we have to resort to history to evaluate how these developments will be developed. As such, we will do a theoretical exercise and try to compare 3D printing with the shared use of digital multimedia files. Although the differences between both technologies are many, the example of multimedia exchange remains our best reference point in terms of the interaction between intellectual property and the Internet, and the logic behind both cases is the same: a finished product can be reduced to a digital file and sent over the Internet to be recreated elsewhere without the authorization of the rights holder.

As bandwidth availability increased in the early 2000s, so did the viability of point-to-point file sharing, something that was first attempted on a large scale using Napster software. Although digital music files were already commercialized since the beginning of the Internet, the possibilities offered by high-speed connections and the larger hard drives in the computer reach their optimum point for technology to take off. Popularity increased, and instead of partnering with Napster to make the transition from illegal trade to a more sustainable model, the industry decided to sue it so that

it did not exist.

While many users were primarily interested in getting free music, others liked the flexibility of having access to music anywhere — they could record tracks freely on CDs and could easily transfer tracks between devices. This finally turned out to be true with the successful launch of the iTunes service (Knopper, 2009). It is known that the intellectual property industry handles digital issues with an aggressive approach. Video and music transmission services have been instrumental in reducing online multimedia piracy, particularly the decline in peer-to-peer transactions, although for a long time such solutions were deemed unviable from the industry's point of view until it was shown that the ease of access was what many customers wanted, not necessarily the zero price tag (Nevola, 2017).

According to an article published by the World Intellectual Property Organization (Malaty and Rostama, 2017), existing laws are sufficient to accommodate 3D printed objects, suggesting that international agreements on copyright and industrial design protect almost all aspects that innovation and additive manufacturing may require. What stands out, from his point of view, is the question of the responsibility of intermediaries, to question how responsible would be the owners of the digital file platforms or the printing machines of illegal activities. They go one step further by suggesting the digital fingerprinting of the models, which will be identified at a basic level through cooperation with 3D printer manufacturers, which are more blocked when forming partnerships with distribution platforms.

In other words, if things develop as they claim, technology will be neutralized from the start, populated by patent trolls, overproduced, and prices will be dictated by global standards from the north. It is not a vague need for a lawless paradise for 3D printing, but it is necessary to bear in mind that this technology will create, for the first time a truly global market, in which a product can be instantly transferred from one place to another with minimal environmental impact, and produced on demand to meet the needs of specific populations. This will entail complex intellectual property implications of multiple layers that cannot simply conform

to current laws without taking into account the particularities of the technology. Imposing strict regulations in the market will invariably lead to 3D printing by the same path that other recent technologies have undergone: abrasion with the application of the law, gray markets and massive piracy. It is a prerequisite that solutions are negotiated to accommodate the needs of developing countries, which are not the same as those of developed countries. The intellectual property industry will have, even if this is achieved through force, to accept the fact that the global south not only seeks to have goods for free, but the disparity of income is so high that establishing prices in such markets is much more complicated than just calculating the highest price that a plot of the population is willing to pay for a certain product.

This will help avoid the need for extreme action by countries in a disadvantaged position and create a better overall environment for 3D printing. If this does not happen, the situation could end up turning in the same way as when Brazil, pressured by the increase in prices forced by international pharmaceutical conglomerates, opted to break patents on AIDS drugs and produce them nationally, leaving patent holders out of the loop. This, in turn, led other countries in the south of the world to look for similar alternatives, creating a vast market of generic medicines that were still subject to patent law according to international agreements (The Economist, 2001).

31.5 Conclusion

As we can see, the implications for the adoption of additive manufacturing processes are not few. It's important that we be attentive as their development evolves, because again and again the world seems to have underestimated the effects of existing technologies, only to notice them with amazement after they rush to the global stage, and the battle becomes a reaction in instead of finding proactive strategies to better accommodate innovations.

The developing world will benefit from the next productive revolution, provided it establishes a clear perception on how to benefit from it in a sustainable and scalable way. This is necessary at the individual level, and it is not an unattainable goal in any way,

since there are already non-state actors strategically positioned within forums and arenas where such issues are beginning to be discussed.

While the future governments may or may not be aligned with these objectives, the international community involved in technical processes and policy formulation shares the collective responsibility to act as vectors of information, working in conjunction with local media, schools, academic institutions, associations commercial and all available places. Educate proactively and help create a connected synthesized existence worthwhile for all of us.

31.6 References

Chow, E. K. (2018). China's War on Poverty Could Hurt the Poor Most. Foreign Policy, 2018. Disponivel em: <http://foreignpolicy.com/2018/01/08/chinas-war-on-poverty-could-hurt-the-poor-most/>.

CIA. (2016). Country Comparison: Exports. The World Factbook, 2016. Disponivel em: <https://www.cia.gov/library/publications/the-world-factbook/rankorder/2078rank.html>.

Cornell University (2013). Bioengineers, physicians 3-D print ears that look, act real. Cornell Chronicle. <http://news.cornell.edu/stories/2013/02/bioengineers-physicians-3-d-print-ears-look-act-real>.

Delanda, M. (1991). War in the Age of Intelligent Machines. New York City: Zone Books.

Ford, S.; Despeisse, M. (2016). Additive manufacturing and sustainability: an exploratory study of the advantages and challenges. Journal of Cleaner Production, Cambridge, v. 137, p. 1573-1587.

Grose, T. (2018). The Worker Retraining Challenge. U.S. News, 2018. Disponivel em: <https://www.usnews.com/news/best-countries/articles/2018-02-06/what-sweden-can-teach-the-world-about-worker-retraining>.

GSMA. (2016). Mobile Internet Users in Latin America to Grow by 50 Per Cent by 2020, Finds New GSMA Study. <https://www.gsma.com/newsroom/press-release/mobile-internet-users-in-latin-america-to-grow-by-50-per-cent-by-2020-finds-new-gsma-study/>.

Harding, X. (2016). Feed Your 3D Printer Recycled Plastic. Popular Science. <https://www.popsci.com/feed-your-3-d-printer-recycled-plastic

Itamaraty. (2016). O comércio Brasil-Japão em 2015. Invest & Export Brasil. <http://www.investexportbrasil.gov.br/o-comercio-brasil-japao-em-2015>.

Knopper, S. (2009). Appetite for Self-Destruction: The Spectacular Crash of the Record Industry in the Digital Age. Berkeley: Soft Skull Press.

Koslow, T. (2017). 3D Printed House – World's 35 Greatest 3D Printed Structures. All3DP. <https://all3dp.com/1/3d-printed-house-homes-buildings-3d-printing-construction>.

Makerbot Thingiverse. (2018) About. Thingiverse. <https://www.thingiverse.com/about>.

Malaty, E.; Rostama, G. (2017). 3D printing and IP law. WIPO. <http://www.wipo.int/wipo_magazine/en/2017/01/article_0006.html>.

Nevola, J. (2017). Internet Piracy: The Effects of Streaming Services and the Digital Marketplace. Science and Technology Law Review. <http://stlr.org/2017/11/14/internet-piracy-the-effects-of-streaming-services-and-the-digital-marketplace/>.

Organización de las Naciones Unidas (ONU). (2013). Impacto de los desastres en América Latina y el Caribe 1990-2011: tendencias y estadísticas para 16 países. UNISDR. [S.l.], p. 72.

Organización de las Naciones Unidas (ONU). (2014). World hunger falls, but 805 million still chronically undernourished. Food and Agriculture Organization of the United Nations. <http://www.fao.org/news/story/en/item/243839/icode/>.

Organización Mundial del Comercio (WTO) (2016). Trade Profiles – China. World Trade Organization. Disponivel em: <http://stat.wto.org/CountryProfile/WSDBCountryPFView.aspx?&Country=CN

Rundle, G. (2014). A Revolution in the Making. Melbourne: Affirm Press.

Sharma, R. (2018). Bitcoin Has a Regulation Problem. Investopedia. <https://www.investopedia.com/news/bitcoin-has-regulation-problem/>.

Shaxson, N. (2011). Treasure Islands: Tax Havens and the Men Who Stole the World. London: The Bodley Head.

Standage, T. (2014). The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-Line Pioneers. New York City: Bloomsbury USA.

The Economist. (2001). Brazil and AIDS drugs: A cure for high prices. The Economist. <http://www.economist.com/node/623985>.

Ventola, L. (2014). Medical Applications for 3D Printing: Current and Projected Uses. Pharmacy and Therapeutics, Yardley, v. 39, n. 10, p. 704-711, oct. 2014.

Watkin, H. (2016). MakerBot Milestone: 100,000 3D Printers Sold Worldwide. All3DP. <https://all3dp.com/makerbot-milestone/>.

Wiggers, K. (2017). From pixels to plate, food has become 3D printing's delicious new frontier. Digital Trends. <https://www.digitaltrends.com/cool-tech/3d-food-printers-how-they-could-change-what-you-eat/>.

POSTFACE

32 The Principles that Guarantee a Free, Open and Inclusive Internet for All People and Social Groups

Edison Lanza

Note: this article was prepared based on the thematic reports of the Special Rapporteurship for Freedom of Expression of the IACHR on the Internet and freedom of expression published in 2013 and 2016, whose citations are included at the bottom of the page.

Abstract

This Afterword analyzes the evolution of the protection of freedom of expression and human rights on the Internet in international law. The digital environment has made it easier for citizens to express themselves freely and openly, and offers unbeatable conditions for innovation and the exercise of other fundamental rights such as free association, the right to culture and education. However, the online environment has become increasingly complex in terms of challenges to the exercise of these rights and the free flow of information, including the privacy of individuals. In regards to the tproblems linked to the equitable and universal access to the Internet, in recent years they have been related to the legal regime of intermediaries -which support the existence of public space and a good part of the operation of the network-; the challenge of maintaining the network neutrality with respect to content and applications; the phenomenon of the storage and handling of huge amounts of personal data in the network, for security purposes or online surveillance. This afterword seeks to systematize some of the responses and perspectives from the perspective of human rights, with emphasis on the inter-American legal framework.

32.1 Introduction

The Internet has exponentially increased the capacity of people to receive, search and disseminate information and opinions. The

new ways of information and communication are related to the ubiquitous and open nature, speed and global reach at a relatively low cost of this global network, which allows the individual and collaborative creation of content, the exchange of ideas and information, and a permanent collaboration to solve social, economic, cultural and environmental problems. The digital space has also been a catalyst for digital commerce, innovation and the expansion basis of a large number of economic activities.

In the digital environment, anyone can be an author, receiver and publisher of information. Intellectuals work and offer their opinion and innovative applications. This represents a form of democratization and decentralization of the freedom of expression right, where public discourse ceases to be moderated exclusively by professional journalists, political and social leaders, or by traditional media. The new expressive freedoms also open new capacities for communication, organization and mobilization, and new possibilities to innovate and generate economic development. This capacity of digital networks and their direct connection with the enjoyment of human rights is giving rise to new debates about the right of people to be connected to the Internet without interference, and even the right to access radio spectrum for common use of communities[609].

In terms of the inter-American human rights system, the freedom of thought and expression, defined in Article 13 of the American Convention on Human Rights, includes the right to seek, receive and disseminate information and ideas of all kinds, without distinction of borders. This right includes artistic expression, written, oral, and printed or any other means of communication. The rules to impose limitations on this right are established in paragraphs 2 to 5 of said article. Within these rules it is emphasized that there can be no prior censorship, if not the imposition of responsibility after the expression is made and in all cases any restriction must comply with the "tripartite test" which requires: 1) that the limitation to be imposed is clearly and precisely defined in a formal and material law which is aimed at achieving imperative objectives

609 Network Self-Determination and the Positive Externalities of Community Networks, Luca Belli (2017).

that are authorized by the Convention;2) that the limitation meets requirements of necessity and suitability to achieve those objectives and; 3) that the limitation is strictly proportional to the purpose pursued. Finally, the responsibilities that are established must always be ordered by an independent and impartial judge or authority, together with the guarantees of due process.

The Special Rapporteurship for Freedom of Expression of the Inter-American Commission on Human Rights (CIDH), together with experts from all systems for the protection of human rights, has maintained as a general principle that *"Freedom of expression applies to the Internet in the same way as to all media*[610]*"*. This implies that any restriction to the exercise of this right on the Internet must follow the standards that have just been explained. In particular, the Office of the Special Rapporteur has emphasized that, when establishing measures that may impact the Internet, the characteristics that make the media a unique space for the increasingly democratic, open, plural and expansive exercise of the Internet must be taken into account the freedom of expression[611].

The growing expansion of this medium in the world and in the Americas has brought, in addition to better opportunities for the exercise of fundamental rights and freedoms, social benefits and inclusion. The due development of these benefits depends on policies and practices that are based on the respect and guarantee of human rights. Within the latter, freedom of expression plays a special role, since it enables the exercise of other rights.

The Inter-American Human Rights System is the international system which provided the greatest scope for freedom of thought and expression and the one that admits the least restrictions, as it arises from the comparison between Article 13 of the American Convention on Human Rights and the protection of freedom of expression in other international treaties, which the Inter-American Court of Human Rights will carry out on several occasions[612].

610 Joint Declaration on Freedom of Expression on the Internet (2011).

611 IACHR. (2013).

612 See in this regard paragraphs 45 and following of Advisory Opinion 5/85 of the Inter-American Court of Human Rights on Compulsory Membership in the Association of Journalists.

This has been possible under a legal framework that seeks to reduce restrictions on the free flow of information, opinions and ideas. According to the Inter-American instruments, freedom of expression is the "cornerstone" of democratic societies, as well as being fundamental for advancing the objectives of sustainable development established by the United Nations and a tool for the exercise of other human rights.

The IACHR and its Office of the Special Rapporteur have highlighted three main functions that freedom of expression fulfills in democratic systems: 1. It is an individual right that reflects the virtue of thinking of the world in its own way and communicating with each other; 2. As a means to deliberate in an open and uninhibited manner on topics that are of public interest; 3. As an instrument for the exercise of other rights, such as political participation, religious freedom, culture, education, equality, among others. In addition, both the IACHR and the Inter-American Court have recognized that freedom of expression has an individual and a social dimension, interrelated. The guarantee of both dimensions must be full and simultaneous.

32.2 Free and open internet

In accordance with the guarantees mentioned here, as a result of the combination of the principles and the inter-American legal framework on freedom of expression and the importance of the Internet for the exercise of this and other fundamental rights, the Rapporteurship has emphasized that the development of public policies and the actions of individuals in the network must adapt to some specific principles, which have allowed the functioning of a free and open Internet in most of our hemisphere.

Among some of the mentioned principles there are the following: openness and universal access, network neutrality, privacy protection to share ideas and express themselves in the network. As this is a relevant issue, we will also address, in the conclusions of this article, the specificity that intermediaries of the private sector have in the network. A multitude of private intermediaries (providers of Internet access, web platforms, mobile applications, etc.) make it possible for us to use the Internet permanently — therefore, the applicable legal regime plays a fundamental role in this field.

These special characteristics must be taken into account by the various agencies that make up the structure of the state at the time of establishing any measure that may impact the Internet. The following is a detailed analysis of each of these principles, as well as the legal status of intermediaries in the private sector that make it possible for the Internet to function as a public space, for the purpose of better understanding it.

32.2.1 Openness and universal access

The concept of openness and freedom in the network is explained by the development of technical standards, such as interoperability, open application interfaces, documents, text and open data, as well as in the absence of limitations or obstacles that artificially favor monopolies or archaic platforms. Openness and universal access are two fundamental principles that are reinforced to maintain a free, open and inclusive Internet.

One of the axes that guarantees freedom on the Internet and openness is the principle of net neutrality.

Access to the Internet is a condition *sine qua non* for the effective exercise of human rights today, especially the rights to freedom of expression and opinion, association and assembly, education, health and culture; therefore, a fundamental principle is that it must be guaranteed universally through measures that close the digital divide and infrastructure development policies.

Despite the commitments and efforts of the States in the region, currently in the Americas a third of the population is without an Internet connection. This lack of access increases vulnerability and deepens inequality, which perpetuates the exclusion of many people. If, in addition to the above, the digital transition of broadcasting services is carried out without ensuring access to this type of service, poor, isolated and remote communities may be adversely affected.

The Office of the Rapporteur believes that expanding access and closing the digital divide goes hand in hand with the need for states to ensure that private actors do not impose disproportionate or arbitrary barriers to accessing the Internet or using their main services.

In the same sense we must call attention to the application of states of exception or administrative policy measures. The interruption of Internet access to entire populations or segments of them is a disproportionate measure for the exercise of the right to freedom of expression and the preservation of democratic societies. Temporary or partial blockades affect the exercise of human rights online.

In this sense, States must develop long-term public policies and plans in order to develop the necessary physical infrastructure to avoid the arbitrary exclusion of certain sectors, and to elaborate broadband plans and measures that allow the development of the mobile Internet.

The digital literacy of the different groups that make up a society is also a fundamental component of the principle of universal access and a particularly necessary measure to protect and guarantee the rights to equality and non-discrimination. Differences in the capacities to use information technologies constitute a gap in knowledge. This component refers to the set of skills, knowledge and attitudes that a person needs to function within the information society. The ultimate goal is that they can *"Use technology effectively, developing new social and economic opportunities within the framework of their society*[613]*"*.

In addition to considerations of universal access, States must also adopt positive differentiation measures to allow the effective enjoyment of this right to people or communities that require it due to their circumstances of marginalization, poverty, vulnerability or discrimination.

This includes, among others, access to technology centers for some communities, inclusive pricing structures and training efforts in poor rural sectors and among the elderly population. In the same sense it is worth mentioning the phenomenon of community networks and the role these initiatives can play in expanding Internet access in communities, but also in the promotion of freedom of expression, digital literacy and the development of new applications, services and local content[614].

---

613 Pan American Health Organization (PAHO). Conversations about Health. (2014).

614 See Luca Belli (Ed.) (2017). Community networks: the Internet by the people, for the people. Official Outcome of the UN IGF Dynamic Coalition on Community Connectivity. FGV Direito Rio. <http://bibliotecadigital.fgv.br/dspace/handle/10438/19401>.

Similarly, instances of online discrimination have been documented to the detriment of particularly vulnerable groups, including women, children, the LGBTI community (Lesbians, Gais, Bisexuals, Transsexuals and Intersex), migrants and people with disabilities, among others. States must adopt measures to promote equality and non-discrimination, prohibiting hate speech that incites violence, documenting instances of discrimination and promoting tolerance through social training and education programs.

It is necessary to emphasize that linguistic plurality is a necessary condition to achieve full access to the Internet under conditions of equality and without discrimination. In the development of the knowledge society, the creation, diffusion, preservation and accessibility of local content should be prioritized, in several languages and formats on all topics – especially scientific, educational and cultural. The translation of websites in several languages is a step forward to guarantee a truly global society.

As the Special Rapporteur on cultural rights of the United Nations has expressed, *"The extremely unequal distribution of literary works published in different languages is a major barrier to the right to participate in the cultural life of linguistic communities without an important editorial market*[615]*"*. While there are online translation services that have been perfected in recent years, they do not constitute effective solutions to this problem.

32.2.2 Network neutrality

The principle of network neutrality is a necessary condition for exercising freedom of expression in the Internet. It also enables innovation and generation of content, applications and services in a decentralized manner, without authorization, licenses or permits. According to this principle – which allows to maximizes the utility of networks – all data packages must be treated in a non-discriminatory way[616].

However, the principle of net neutrality may be subject to exceptions, when strictly necessary and proportional to preserve the integrity

615 United Nations. (2014). Para. 68.

616 See <https://www.networkneutrality.info>.

and security of the network; to prevent the transmission of unwanted content by express request free and not encouraged – of the user – and to temporarily and exceptionally manage network congestion. In the latter case, the measures employed must not discriminate between types of applications or services[617]"

Hence, the Internet is described in practical terms as a 'dumb' network whose specialization ('intelligence') is generated at the extremes. The platform or application operates at one end of the network, and its contents are moved across the network and divided into data packets without being discriminated against. Such packages are reset again in the destination depending on the recipient, the platform or application they use.

The treatment of data and traffic on the Internet should not be subject to discrimination according to the source, content, application or device. The network neutrality guarantees the freedom of access and choice of users. It allows them to send and receive information or offer any content, application or legal service through the Internet without conditions or discrimination, blocking, filtering or interference.

The States must guarantee the validity of this principle through appropriate legislation. Several countries in the region have already adopted laws that enshrine the principle of net neutrality, including Argentina, Brazil, Chile, Colombia, Peru and Mexico. Additionaly, the National Telecommunications Commission of Paraguay endorsed the principle of net neutrality.

The Federal Communications Commission in the United States (FCC) had also protected this principle from the *Open Internet Order* of 2010, and adopted a particularly protective framework in 2015 under the limitation imposed on intermediaries not to block, not slow down some content over others or enable faster lines on the Internet in order to favor some applications over others. However, in December 2017 a new integration of the council of the agency eliminated these requirements for the Internet service providers, and only maintained the obligation to inform users

617 IACHR. Annual Report 2013. Report of the Special Rapporteur for Freedom of Expression. Chapter IV(Freedom of Expression and the Internet). OEA/Ser.L/V/II.149. Doc. 50. 31 December 2013. Para. 30.

about the network management. At this time, general attorneys of several states of the United States have challenged that decision, while some states passed regulations that oblige Internet services providers to respect network neutrality in their states.

Together with David Kaye, Rapporteur for Freedom of Opinion and Expression of the United Nations, in an opinion that we sent to the FCC during the review process of the network neutrality rule, we recall that this principle is fundamental for innovation and freedom of expression on the internet[618].

Another example regarding how this principle may be affected, is related to the offer of 'zero rating' Internet plans in 2015, designed primarily for the mobile Internet service, through which companies offer access to certain applications without constituting an expense in the user's data plan. There are *zero rating* plans in different countries of the region such as Chile, Colombia, Brazil, Bolivia, Ecuador, Panama and Paraguay[619].

Although the doctrine is divided in regard to the impact of the plans of *zero rating* in network neutrality, these policies should be evaluated in light of the principle of non-discrimination and freedom of expression. On the other hand, in any case States may replace their universal access to the Internet policies or plans *zero rating*. The simple substitution of access policies for such programs is incompatible with the development objectives of the United Nations and with the obligation of States to promote and protect human rights on the Internet.

Of course, the network neutrality principle may be subject to exceptions, when it is necessary and proportional to guarantee the integrity and security of the network, or to prevent the transmissions of contents not expressly desired by the user. Even in the case of congestions or technical problems, the measures should not discriminate applications or services.

Transparency in the network´s management is fundamental to guarantee the principle of network neutrality. States should require Internet intermediaries to be transparent about the practices

618 See summary of the letter at: <https://mobile.reuters.com/article/amp/idUSKBN1EE2DA?twitter impression=true>.

619 See <https://www.zerorating.info>.

employed in data traffic management. This information must be available to users in an affordable format.

32.2.3 Privacy

The respect for privacy is also a guiding principle of the digital environment. The right to privacy, according to which no one can be subject to arbitrary or abusive interference in private life, in family, in home or in correspondence, is important for exercising the right to freedom of expression on line. The violation of the privacy in communications has an inhibitory effect and affects the full exercise of the right to communicate. Therefore, this right must be protected by law and strictly promoted through public policies.

With the Internet having the technical capacity to gather, store and exchange personal information provided by digital technologies, new challenges have been generated in the protection of privacy. Social networking companies are based on a business model that offers 'free' services in exchange for ownership of the data generated by users. Thus, the use of the Internet necessarily implies the generation of data and 'digital traces'.

This complicates the right of people to determine when, how and to what extent information about themselves is shared. The increasing power of computer processing, together with the growing diffusion and branching of data runners, allows to gather information from multiple sources, process and re-process it and then sell this information. It is clear that the business model of the most successful companies directly affects the right to privacy.

New technologies also create the possibility of locating and tracking personal data, something that was not possible before. Each computer, mobile phone or other device connected to the Internet has a unique address (IP address) that provides a specific identifier to the device and allows its tracking. The GPS systems, additionally, are able to track through different applications the exact location of a person. On the other hand, there are various tools to extract personal information from the user or to identify it, such as *cookies* and the webs *bugs* or *beacons*.

The protection of privacy on the Internet also implies the adoption of a broad notion of personal data, which includes any data to identify individuals. It is essential to develop data protection regimes that regulate the storage, processing, use and transfer of personal data, either between state entities or between third parties. Due to the cross-border nature of the Internet, the need to regulate data processing is not limited to the national level.

The States must adopt policies to regulate the processing of data, including the storage, analysis, and disclosure of personal data, except when they are legitimized to do so or there is informed consent of the affected person. In addition, they must adopt positive measures to educate people about their rights and the legal conditions for the processing of personal data (collection, storage, processing or disclosure of data).

In this field, transparency is also fundamental regarding the legislation applicable to the handling of data by both the State and the private sector. It is fundamental that people can access the information stored about themselves, enjoying the right to update it, correct it and, if necessary, eliminate it when necessary.

The right of access and the obligation of transparency regarding personal data stored by the State also includes biometric data, which allows *"The systematic recognition of individuals based on their behavioral and biological characteristics*[620]*"*. The systematization of all these data, combined with other sources of behavioral information, allows, under a probability system, to identify people.

When States, in the framework of their security functions, perform data collection tasks, they must observe strict criteria of necessity and proportionality when determining what data they collect and how they do it. They should establish protocols around the collection, respectful of human rights, particularly the principles of legality, necessity and proportionality and guarantee the right of access to information regarding the policies and practices in force in the matter. This process must be subject to both administrative and judicial control.

620 Association for Civil Rights.

32.2.3.1 Surveillance, monitoring and interception of communications

Individualized surveillance is generally covered by criminal proceedings or other types of investigations, and includes the interception or monitoring of communications. Massive surveillance of communications and data, involves the interception and inspection of entire cables, networks, or equipment, or the purchase of data from servers or intermediaries from a third party.

Technologies developed in recent decades have simplified and dramatically reduced the costs – both human and financial – of digital surveillance. Hence, its use has increased radically. Considering these and other dangers that technological developments bring, the commitment that States must assume to protect the privacy of citizens is higher.

Surveillance on the Internet, in any of its formats or nuances, constitutes an interference in the privacy of individuals and, if exercised illegitimately and in a massive way, may also affect the rights to due process and a fair trial to the freedom of expression and access to information.

Not all interference is *per se* illegitimate. There are exceptional cases that justify different levels of interference according to the circumstances. Terrorism and the fight against organized crime, for example, suppose a state obligation of prevention and protection that constitutes a legitimate objective for the exceptional and supervised use of surveillance technologies and mechanisms. However, States must guarantee the adequacy of these measures to human rights.

In the same line, the systematized collection of public data – voluntarily exposed by the owner of such data- such as blog posts, social networks, or any other intervention in the public domain – constitutes an interference in the private lives of people. The fact that the person leaves public traces of their activities does not enable the State to collect it systematically, except in the specific circumstances when such interference is justified. It is necessary, in those cases, to analyze it in the light of the tripartite test: the measure must be legal, in a formal and material sense, necessary and proportionate.

In view of the intrinsic risk of abuse of any surveillance system, these measures should be based on a particularly precise legislation, with clear and detailed rules. The objectives according to which monitoring or interception of communications is enabled must be expressly stated in the law and in all cases it must establish the need for a prior court order. The nature of the measures, as well as their scope and duration, must be regulated, establishing the facts that could give rise to those measures and the competent bodies to authorize, implement and supervise them.

Several States in the region have acquired new surveillance technologies which procurement, use, disposal and supervision processes lack sufficient regulation or dissemination. Laws and policies regarding the nature, scope, and implementation of interception and monitoring mechanisms must be public and the State is obliged to apply the principle of maximum disclosure in accessing that information. This covers both the policies and practices around electronic surveillance, as well as the acquisition, development, or updating of the systems available for this purpose. In recent years the Office of the Special Rapporteur has warned on several occasions about the lack of transparency and adequate regulation in the acquisition of this type of surveillance software and malware by several states in the region, as illustrated by the cases of Haking Team and Pegasus[621].

In establishing a restriction on access to information on surveillance systems, States must demonstrate the need for any measure to keep certain information secret in order to protect national security and public order. The concept of national security cannot be interpreted in any way and must be defined from a democratic perspective.

It should be reiterated that the surveillance measures must be ordered by a competent or independent and impartial judge or court, and the order must be duly founded and observe due process.

621 See in this regard: Special Rapporteurship expresses concern over allegations of espionage by journalists and human rights defenders in Mexico and urges a full and independent investigation, July 12, 2017 (http://www.oas.org/es/cidh/expresion/showarticle. asp?artID=1069&lID=2); Special Rapporteurship expresses concern over the acquisition and implementation of surveillance programs by states in the hemisphere, July 21, 2015 (http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=998&lID=2).

Intermediaries, on the other hand, have a particularly important role in this matter. States often depend on the collaboration of these private actors, and there are numerous initiatives tending to force them to keep records, or to control or monitor the activities of their users. The private sector must disseminate information regarding the processes they implement, indicating at least in aggregate the number and scope of the requests they receive to deliver data under official request[622].

32.2.3.2 Anonymity and encryption

For many individuals, an opinion expressed on the Internet can lead to reprisals. That is why States have the obligation to respect anonymous discourse as an exercise of privacy and freedom of expression, and only exceptionally require authentication or reliable identification of the person expressing it, applying a proportionality criterion.

The private sector must also protect anonymous speech, for example by avoiding imposing on its platforms identification requirements that the law itself does not require. Anonymity protects the privacy of individuals and enhances freedom of expression by allowing unidentified participation in the public debate.

Notwithstanding the foregoing, States may take measures to identify a person in the framework of a judicial investigation in the terms set forth in this report. Anonymity can be lifted, for example, when the speech is not covered by the right to freedom of expression, as is the in the case of the speech that makes propaganda in favor of war, the apology of hatred that incites violence, the incitement to genocide and the sexual exploitation of minors.

To the same extent, encryption is a resource aimed at protecting the privacy of information in the digital age, and consists of the coding of data so that only the recipients can access it. The measures that restrict encryption then reduce the ability of people to protect themselves against unlawful invasions of their privacy. These

622 The Annual Reports of the Office of the Special Rapporteur for Freedom of Expression in recent years account for a large number of legal initiatives, many of them already approved, which contain provisions aimed at determining the obligation of telecommunications companies and platforms to store data during certain period of time for security purposes, for example.

measures should not be adopted by States except exceptionally and as long as they are legal, necessary and proportional.

32.2.4 Big Data

The immense amount of data generated in the network, which can be stored, managed, analyzed and systematized in search of trends and profiles, constitutes a new challenge for human rights.

The collection and analysis or "mining" of data would make it possible to assess needs and social trends that are potentially useful for the adoption of more and better public policies in order to guarantee the human rights of people. But, to the same extent, a large number of private companies are dedicated to the development of technologies that allow them to analyze data on a large scale to assess market trends, preferences, demographic profiles and political and cultural inclinations, among many other variables.

Many of the technologies that are being used not only allow the objective analysis of data and trends, they also allow the identification of the users within the analyzed critical mass, and allow the generation of detailed profiles of each individual with risks of discrimination and arbitrariness. States should ensure that both technology and developments in the public and private spheres related with *Big Data*, guarantee the protection of human rights on the Internet.

32.2.4.1 Internet of things

In the near future, objects will be able to communicate with each other without human intervention. The Internet will then become a physical experience of objects that will constantly gather information about people: an *Internet of Things*.

The Office of the Special Rapporteur recognizes that the rapid technological change that characterizes this period makes it difficult to anticipate the social consequences of a technology. It is up to the States, on behalf of their citizens, to understand what the new technologies imply in terms of public policies and to ensure that they work in the public interest with sufficient protections for users and their human rights.

32.3 Conclusions: role and legal regime of intermediaries

In fact, the Internet has been developed and operated by a series of private companies that perform different functions, although its character as a global communication platform makes it a public space. Therefore, Internet governance must be exercised under the principles of a public resource and not simply as a matter of private contracts.

The transmission of content on the Internet depends on the intermediaries. In general terms, intermediaries are "any entity that permits the communication of information from one party to another[623]". However, the legal definition of 'intermediary' may differ between jurisdictions or between countries. For practical purposes, we consider as intermediaries to the Internet service providers search engines, blogging services, e-commerce platforms, web servers and social networks, among others.

One of the measures that can affect the performance of intermediaries on the Internet is the liability regime that is legally imposed on third-party content. The liability regime is essential to generate the incentives adequate for the protection and guarantee of human rights. In all cases, the liability regime must follow the tripartite test that allows limitations of fundamental rights only when the principles of legality, necessity and proportionality, established by the inter-American human rights system are respected.

No actor that limits itself to offering Internet technical services such as access, searches or information preservation, must be responsible for the contents generated by third parties that are disseminated or stored in their services. The foregoing applies, provided that the intermediary does not intervene in said contents or refuses to comply with a court order when it is able to do so. In the same sense, subsequent responsibilities should be imposed on the authors of the content and not on the intermediaries.

The "strict" liability that the intermediary holds as responsible for any content considered illegal in its platform is incompatible

623 See UNESCO (2014: 19).

with the American Convention because it is disproportionate and unnecessary in a democratic society. This type of regimes promotes the monitoring and censorship of intermediaries for their own users. On the other hand, conditioned liability systems are more closely aligned with international standards, as long as they comply with the principles of necessity and proportionality. Under the conditioned responsibility, the intermediary is offered a "safe harbor" from any legal liability as long as it complies with certain specific duties.

On the other hand, it is worth noting the existence of the "notification and withdrawal" systems, within which the intermediary must withdraw the content once notified of its existence; the system of "notification" in which the intermediary must notify the author of any complaint received regarding its contents; and the "notification and disconnection" system, in which the intermediary will disconnect the user when, after notifying him, he does not remove the content reported. These models of conditioned responsibility do not impose a duty to monitor or filter content in a proactive manner. However, they do not always respect the right to due process and minimum guarantees, while transferring to the intermediary the responsibility of the state to analyze and decide on the legality or illegality of the content susceptible to removal. For the Office of the Special Rapporteur, these models will be compatible with the American Convention insofar as they protect freedom of expression and do not impose ambiguous or disproportionate obligations.

The Manila Principles on Liability of Intermediaries[624], proposed by civil society organizations from around the world, propose a frame of reference of minimum guarantees and good practices for States in the area of responsibility of intermediaries on the basis of international instruments on human rights.

It should be noted that taking into account the global and transnational reach of the Internet, States should aspire to achieve uniformity in the rules that govern the responsibility of intermediaries as a fundamental aspect to maintain a free, open

624 View <https://www.manilaprinciples.org/es>.

and global Internet. When deciding questions of responsibility, the competent judges should be those who have the closest contacts with the case, attending where the victim resides, where the content is originated, or where the author resides. The judges have the responsibility to avoid what is known as "defamation tourism" or *forum-shopping*, declaring themselves incompetent when there is no demonstrable substantive harm in their jurisdiction.

This issue has been repeatedly raised in judicial decisions regarding the so-called 'right to be forgotten' (see below), in which a judge in a country orders the de-indexing of a specific search result not only from the platform linked to competent jurisdiction, but also from other countries (or even globally). This could lead to an extraterritorial application of a national court order and raises complex questions about the future of Internet jurisdiction and its interaction with national sovereignty.

32.4 References

Asociación por los Derechos Civiles (Mayo de 2015). Si nos conocemos más, nos cuidamos mejor: Informe sobre políticas de biometría en la Argentina. <https://adcdigital.org.ar/wp-content/uploads/2016/01/Si-nos-conocemos-mas.pdf>.

CIDH. (31 de diciembre de 2013). Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo IV (Libertad de Expresión e Internet). OEA/Ser.L/V/II.149. Doc. 50.

Declaración conjunta sobre libertad de expresión en internet. (1 de junio de 2011). <https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&lID=2>.

Naciones Unidas. (24 de diciembre de 2014). Consejo de Derechos Humanos. Informe de la Relatora Especial sobre los derechos culturales, Farida Shaheed. UN Doc. A/HRC/28/57.

Organización Panamericana de la Salud. (2014). Conversaciones sobre Salud. Gestión de información, diálogos e intercambio de conocimientos para acercarnos al acceso universal a la salud. Washington DC.

UNESCO. (2014). Fostering Freedom Online: The role of internet Intermediaries. Unesco Series on internet Freedom

This book celebrates the ten-year anniversary of the *South School on Internet Governance*. The authors of this volume are (in alphabetical order): Carlos Álvarez, Pablo Bello Arellano, Horacio Azzolin, Carlos F. Baca-Feldman, Filipe Batista, Sebastian Bellagamba, Luca Belli, Humberto Carrasco Blanc, Adrián Carballo, Olga Cavalli, Vinton G. Cerf, Margarita Valdés Cortés, Nadine Andrade Chorão, Mark W. Datysgeld, Lacier Dias, Danilo Doneda, Raúl Echeberría, Luã Fergus, Pedro Augusto Francisco, Oscar Robles Garay, Raquel Gatto, Agustín Garzón, Julio César Vega Gómez, Jorge Javier Vega Iracelay, Edison Lanza, Cláudio Soares Lopes, Daniela Parra Hinojosa, Maryleana Méndez Jimenez, Peter Knight, Eduardo Magrani, María Álvarez Malvido, Oscar A. Messano, Laura Schertel Mendes, Christian O'Flaherty, Renan Medeiros de Oliveira, Eduardo Molina Quiroga, Bruno Ramos, Karla Velasco Ramos, Andrés Sastre, Vanda Scartezini, Vanessa Fusco Nogueira Simões, Hugo Fusco Nogueira Simões, Christoph Steck, Erick Huerta Velázquez, Nicolo Zingales.

The Internet has become an integral part of the lives of all connected individuals and an essential tool for forming our opinions and enabling us to learn, communicate, socialize, do business and access public services easily and globally. This volume does not intend to comprehensively analyse the evolution and impact of the Internet in Latin America, but rather to offer the elements necessary to understand and question several facets of Internet governance and critically analyse a number of regulatory tools that influence its evolution in the region. This work adopts a multistakeholder approach by including a series of very heterogeneous analyses written by some of the region's most recognised experts from academia, the public and private sectors, civil society and the technical community.

This book confronts different opinions on the governance and regulations of Internet infrastructure, connectivity models, privacy, cybersecurity and technological developments in Latin America. In this sense, the reader may find varied and sometimes divergent opinions, since the purpose of this work is not to offer definitive solutions, but only to share ideas and elements of pluralistic reflection, to help each one to form their opinion in a critical and independent way.

"I am honored to write this foreword to an important and timely book on the challenges posed by today's Internet. This analysis is crucial to understanding the most important governance issues relevant not only to the Americas but also to the rest of the world where the Internet is accessible and especially where it is not yet available."

Vinton G. Cerf, Vice president and Chief Internet Evangelist, Google

"The digital environment facilitated the free and open expression of citizens, providing unbeatable conditions for innovation and the exercise of other fundamental rights such as free association, the right to culture and education and of people's privacy. This book seeks to systematize some of the most relevant issues and offers particularly important answers from the inter-American perspective."

Edison Lanza, Special Rapporteur for Freedom of Expression,
Inter-American Commission on Human Rights

"ICT-related public policies must serve as the basis for social inclusion, respecting cultural and individual and collective thought diversity. This book is essential to understanding the main purpose of Internet Governance: to make bridges respecting the multiple characteristics of behaviour that define us as human beings."

Bruno Ramos, Regional Director of the International Telecommunication Union (ITU)
for the Americas region

Agência Brasileira do ISBN
ISBN 978-85-9597-036-6
9 788595 970366